

Confidential

G Gaming Limited

ISO 27001 Policies & Controls



Exported on 19/12/2024 at 11:30

Confidential

Background Information

Access to this environment and team member controls

Making the template documentation work for your organisation and its stakeholders

Assigned to: Dan Rough

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Cheryl Jones on 29/10/2021 10:14

Categories:

No Categories to display

Added by ISMS Creator on 22/10/2021 at 09:01

Context

Please digest the following high level guidance and ensure that any team member taking ownership for Adopting, Adapting and Adding to your policies, controls and processes is aware of it for a consistent, compliant and joined up management system that everyone in your scope will understand.

Once digested simply submit this activity for approval and approve it yourself as you don't need independent approval for this guidance. Once approved, there is no need to review it again so don't set a reminder either!

A major benefit from the platform is the actual ISMS it creates for you, making life much easier during implementation and ongoing management. To aid that we have also created actionable documentation that is easy to Adopt, Adapt or Add to. All the tools, processes and techniques we have wrapped around the documentation allow you to easily demonstrate that ISMS working - you just need to use them.

If you don't use them and rely on other tools e.g. if you want to keep existing security incident processes/tools, then remember to adapt the documentation accordingly in Annex A 16. Then delete or avoid use of our pre-configured security incident tracker.

Documentation included for your head start

The activities making up the ISO 27001 main requirements and control objectives for Annex A include some or all of the following:

- **An activity description** (like the one in the blue box to the left) - this is effectively what needs answering and is derived from the ISO 27001 standard itself - so you can be confident that you are considering all parts of the standard and not missing anything that could affect certification.
- **A template policy / control you can simply Adopt, Adapt or Add to.** The more significant the % progress indicator on the left, the more that indicates how much or how little effort you'll need to spend on it - i.e. 95% means you should be able to quickly and easily Adopt that approach with very little effort (e.g. the risk methodology and tool set). 0% means it is unique to your organisation and there is no policy template provided per se (as it might send you in the wrong direction for your business). You'll want to ensure that any policy reflects controls and practices around how your organisation wants to operate e.g. [\(A.9.4.2\)](#) is about secure log on - this will be unique to your organisation.

Please remember that just because something is 95% in its description and you can Adopt it easily, you might still have some practical work to demonstrate it in practice e.g. adding your specific risks and treating them - although we have made all that very easy too!

- **High level tips and guidance.** We have included high level tip and guidance where that makes sense to do so. (Please feel free to give us feedback via support if you want more help or feel we can add more tips/guidance in future too).

Please note that the optional Virtual Coach package includes much more depth in the way of videos, guides, checklists, exercises etc. at a small extra cost. If you are new to the standard and ISMS, the Virtual Coach will save you an awful lot more time and money overall as well as help you get even better outcomes.

Editing and amending documentation to reflect your needs

For independent certification e.g. UKAS you need to ensure your documented ISMS reflects your organisations way of working. The auditor should be able to see your ISMS reflects your organisation needs, culture, style and risk appetite.

We encourage you to read the content in each area, then edit and amend them to your needs. This will also show each policy or control as updated by your organisation. Earlier versions will still be saved if you need to come back to it in future (unless you choose to delete it).

Once you are confident you've implemented an area simply remove the tips from the top. Otherwise it might suggest to an auditor that your attention to detail is in question and they may choose to ask even harder questions of your physical practices!

All good auditors will tell you that they want to see the spirit of the standard being applied as well as the actual ISMS being implemented too.

**we encourage pithy policy notes where possible as they are better for ISMS control and easier for stakeholders to digest especially if the optional Policy Pack feature is used. However there are occasions when an uploaded document is better e.g. if it's a very long complex policy/control, has pictures etc - such as the risk methodology, supplier policy etc and no doubt some of your own documented procedures when you get to (A.12.1.1).*

Stakeholder communications and style for policies & controls

Depending on the scope of your ISMS there may be a number of stakeholders who need to understand and comply with your policies and controls. These include staff, key suppliers and perhaps board members, non execs etc. Remember to write your policies and controls in a manner reflective of the audience that needs to understand them and be mindful of policy length, style, tone of voice etc. Our template documentation approach may be fine or it might need some changes by you with that goal in mind. The more you write for that target audience the more likely they are able to read and comply with your expectations.

In addition to exporting/printing your policies off individually or as a whole document, we have developed an optional Policy Pack service that allows you to elegantly publish those policies into your audience in a 'kindle like' manner. Their job of reading and confirming compliance is made simple too - *but they still need to understand the content being published* - and your job of monitoring for assurance and compliance also becomes very easy with that service!

If you are using the Policy Pack feature then a great way to test your content through that audience lens before final publishing is to prepare a Policy Pack and view the content in there. Tip - if you don't already have Policy Packs turned on, ask your ISMS.online rep for a free trial as it also makes the final published policies

much more attractive than the other export/print options even if you choose to export them and share via an existing intranet.

Linked work

No Links to display.

Confirmation of who should access this environment, when and how, their roles, including how access to information is controlled and updated

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 08/03/2023

Status: Completed

Approved by Helen Walton on 26/04/2023 08:23

Categories:

No Categories to display

Added by Helen Walton on 29/11/2022 at 13:39

This environment has been set up to provide easy access to and management for all the relevant policies and controls for the organisation as regards information security and related standards management. It ensures compliance with the various standards and controls expected across ISO 27001 and related certifications.

Membership of the environment is strictly controlled by either:

1. Direct team member access with board membership, because someone is a member of the Management Review Board and may need to approve certain changes in live (which are auditable).
2. Direct team member access for the nominated Security Officer to include admin or management rights (meaning an ability to edit or change the project structure) but not the rights to approve changes unless they are also 1.
3. Associated team member rights to view and access information as a result of membership being granted temporarily by the Management Review Board. All general communications about the ISMS that affect staff and other relevant interested parties who need to access the policies and controls will be conducted in our internal Notion page and announced via the relevant Slack channel.
4. Key partners including third party testing houses, regulators, security consultants or auditors will also be granted read-only access. Currently the third party appointed to audit the ISO will continue to have access between engagements. This will be reviewed annually.

Linked work

No Links to display.

Normative References with Terms and Conditions

Upload your copy of ISO 27001 here for reference

Demonstrate your organisation has access to a licenced copy of the ISO 27001 and 27002: 2013 standards along with any other applicable terms and conditions

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 21/06/2022 15:33

Categories:

No Categories to display

Added by ISMS Creator on 22/10/2021 at 09:01

In order to comply with ISO standard obligations for independent certification you should use this environment to demonstrate that you have access to or purchased the [ISO 27001: 2013 standard](#).

If budget is not so much of an issue or you have particularly complex technical operations you may find [ISO 27002](#) is worth getting access to as well for very specific wording guidance on Annex A controls.

Single licence copies of the standard are not that expensive (typically around £100) however we understand that some libraries and community groups may make these documents available for reading too as part of the membership.

We recommend you upload the documents here if you have purchased them or add a hyperlink / note to show where you were drawing that insight from for the standard if asked by an external auditor.

Documents

 [Cert 140 ISMS.pdf](#) Added: 21/06/2022 Added by: [Helen Walton](#) Version: 1.0

Linked work

No Links to display.

ISO 27001 Requirements - 4.1 to 10.2

4 Context of the organisation

4.1: External and internal issues

The organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome/s of its information security management system

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 12:07

Categories:

No Categories to display

Added by Helen Walton on 29/11/2022 at 13:48

What we do

Background and context to our organisation and its products/services

G Gaming Ltd creates and serves gaming software within the regulated gaming industry. We supply lotteries, casinos and sports books with a variety of games which are certified and run on our own RGS using our certified RNG.

Organisation purpose

- Our purpose is to build games that players love and our customers can rely on
- Given the nature of the information that G Gaming processes and its value, both to G Gaming itself and to G Gaming's customers, the security of information is at the heart of G Gaming's operations. All members of G Gaming are required to familiarise themselves with this policy, to adhere to it, and comply with its requirements.
- There are a range of internal and external issues that need consideration and may affect the intended outcome of our ISMS.

The internal and external issues noted below have been developed through numerous risk identification sessions with the Board and other relevant groups of colleagues. G keeps an up to date Risk Register which informs the risk identification, evaluation, analysis and treatment undertaken in accordance with (6.1) which then leads onto the creation and implementation of appropriate policies and controls for our ISMS.

Internal Issues that might affect the intended outcome for the ISMS

Information (& related Assets)

- *Here we consider and list there high level information and related assets and how they could become issues (align with (A.8.1.1) asset inventory)*

People

- *Failure to retain key staff*
- *Difficulties in recruiting talented staff*
- *Changes to management or personnel in key customers*
- *Rising staffing costs*
- *Staff failing to comply with policies either deliberately or through a lack of awareness.*

Organisation

- *Ownership and structural changes that can cause jurisdictional difficulties*
- *Reliance on third parties*
- *Complexity that can lead to higher costs*

Product/Service

- *Failure to keep up to date with new trends / innovations*
- *Performance issues in products*
- *Vulnerabilities to potential hacks or exploits*
- *Infringement of IP*
- *increased competition*

Processes

- *Failure of internal testing and release processes - allowing vulnerabilities, errors or service problems to affect customers or players*
- *Failure to implement risk management procedure or follow policies*
- *Failure to follow compliance or jurisdictional requirements leading to late or missing audits and renewals*

Systems

- *service outages caused by system failures*
- *failure to upgrade or maintain systems*
- *Miscommunications and misunderstanding in requirements (especially compliance)*
- *Fraudulent hacks on the system or vulnerability exploits on the games*
- *Maintenance of fit for purpose infrastructure, including combination of cloud vs physical servers as required by regulation*
- *Data or privacy breach*

-

External Issues (considered using PESTLE) that might affect the intended outcome for the ISMS

Political

- *Changing attitude to gambling in the various jurisdictions we serve leading to changing regulations (see below)*
- *Distributed teams working cross the world means our staff or closely related third parties in some areas may be at risk: Ukraine, India, Spain, Estonia and UK*

Economic

- *Increase in taxation*
- *Failure of Game performance*
- *Failure to manage cashflow effectively*
- *High fixed costs (increases in infrastructure costs)*
- *Reduced margins (revenue share squeeze) and increased promotional activity at unsustainable rates*

Sociological

- *Increased press or social hostility to gambling*
- *Failure to detect money laundering or fraudulent activities of customers*

Technological

- *Changes in mobile technology (ios/native rules)*
- *Significant changes in device / browser support*
- *New game formats or technical tools*
- *Launch in markets with lower connectivity/ less developed devices*

Legislative/Regulatory

- *Changes in requirements not being picked up or applied correctly*
- *Failure to conduct audits and renewals on time*
- *Repeated changes to rules increasing complexity and costs*
- *Fines or reputational damage*

Environmental

- *Changing costs of power or doing business*
- *Business in environmentally at risk areas*

Linked work

No Links to display.

4.2: Interested parties

The organisation shall determine interested parties (stakeholders) that are relevant to the information security management system and the requirements of these interested parties relevant to information security.

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 12:40

Categories:

No Categories to display

Added by Helen Walton on 25/02/2022 at 11:40

What we do

Interested parties are determined initially by brainstorming with key employees and senior management, then plotted in order to determine how much investment and resource is required, and what impact these interested parties should have on our ISMS.

- The [Interested Parties map](#) is used to document and track our interested parties*.

The [Interested Parties map](#) brings alive the methodology below and is used to illustrate our approach. This offers a level of insight and analysis to help segment and focus attention where it is needed most. The idea is to keep the process simple and not over-engineer or complicate it, it is a basic but effective piece of portfolio management.

Methodology

- **Interested party** - someone, a group or organisation that has a stake or interest in our organisation, its services or the customers we serve, in particular around the information and related assets.
- **Power** - this is the level of power that a stakeholder has from a choice of 1 very low to 10 very high, which is also relative to others, determined from very low to very high. Power includes the capability to influence the Confidentiality, Integrity & Availability of information that affects our purpose, the ISMS and its objectives.
- **Interest** - this is the level of 'day to day' interest we perceive a stakeholder or group of those stakeholders has in relation to their other interests. Again a 10 tier low to high scale is used to help distinguish interested parties. Interest includes their interest around the Confidentiality, Integrity & Availability of information that affects our purpose, the ISMS and its objectives.

The 4 quadrant mapping labels e.g. 'keep satisfied', is an indicative output from the mapping of how to treat the mapped party.

- **Support** - means we have ISMS mechanisms in 'support' of what the stakeholder's interests or requirements are, and our levels of happiness, reflected as follows:

Happy/Green - We have considered the Interests of the party and addressed known risks or aspects around them within the ISMS

Neutral/Amber - The Interests of the party are being addressed but may need to be reviewed in light of other changes in the ISMS.

Unhappy/Red - We have considered the interests of the Party but our risk assessment and broader ISMS does not yet reflect it, so steps need to be taken for that.

Don't know - we need to do more work to establish the needs and interests of the party and then consider whether the ISMS addresses their interests & requirements.

All parties' interests are considered as part of our ISMS. Where relevant they are then factored into the risk assessment and treatment which also informs the creation of relevant policies and controls set out to meet the ISO 27001 accreditation and any related standards we may also follow.

*Our mapped 'interested parties' include those parties who form part of the applicable legislation - these are dealt with collectively in this environment for ease as one stakeholder, but dealt in detail as part of the [applicable legislation risk map](#) where their specific interests are addressed from a risk management perspective. Contracts are also dealt with separately in the relevant areas from a customer, supplier and other important relationship perspective whilst taking into account the relevant ISO 27001: 2013 requirements for example in [\(A.13.2.4 \(Confidentiality or non-disclosure agreements\)\)](#) and [\(A.15\)](#) for supplier activity.

Documents

 ISMS.online Interested Parties 2022_02_25_11-31.pdf	Added: 25/02/2022 Added by:	Helen Walton	Version: 1.0
--	-----------------------------	------------------------------	--------------

Linked work

Risks

AU: Exploitation either deliberate or inadvertent by normal users due to or allowed through: - inadequate policies; their communication; or enforcement (e.g. malfunction voids play) - Low morale or other external factors (e.g. financial/criminal/ethical) encouraging deliberate malicious behaviour - inadequate network security controls - inadequate monitoring & logging of systems, networks and user activity - inadequate use of encryption on internal systems - inadequate vulnerability management in networks and systems - inadequate incident management	Risk map: Risks & Treatments	24
	Project: ISO 27001 Policies & Controls 2022	

4.3: Scope

The organisation shall determine the boundaries and applicability of the information system to establish its scope. Take into account the external and internal issues (4.1) and requirements (4.2) and interfaces and dependencies between activities performed by the organisation, and those performed by other organisations.

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 30/11/2023

Status: Completed

Approved by Helen Walton on 07/05/2024 12:51

Categories:

No Categories to display

Added by Helen Walton on 07/05/2024 at 12:51

What we do

Scope

G Gaming designs, develops and serves real money games in regulated jurisdictions.

Having considered the internal and external issues (4.1) facing us, as well as the requirements from Interested Parties (4.2) and the interfaces and dependencies between activities performed by the organisation and those performed by other organisations, the scope of this ISMS is as follows:

- *To define a policy by which G Gaming's software systems, assets, infrastructure, and computing environment will be protected from threats whether internal, external, deliberate, or accidental.*
- In particular, this takes into account the fact that G is a real-money gaming business which makes it at high risk of external attack both from fraud and manipulation of potential software vulnerabilities, as well as industry-specific risks such as money laundering and proceeds of crime (gambling being viewed as a potential way to launder money). There is also a high risk of internal fraud due to the potential gains of exploiting the software to win real money. These are specific risks to the industry type and our systems have many specific features from how we develop our software to how manage changes to our code or production environment that are designed to work with this. We track these [risks](#), but also record and review any exploits or incidents including those which we have a duty to report to our customers or regulator.
- As a highly regulated industry, there are also specific ISMS requirements that are about compliance with the jurisdictions in which we serve games. These range from how we store and report on critical files within the games, monitor RTP and store data to unique configuration requirements such as top prize limits or spin speed. All these requirements are recorded in our Applicable Legislation and [Jurisdictional Requirements](#) These requirements can also change regularly and staying up to date with such changes as well as implementing them in time is essential to both our own licence and those of our partner operators.
- Given the nature of the information that G Gaming processes and its value, both to G Gaming itself and to G Gaming's customers, the security of information and data classification is at the heart of G Gaming's operations. All members of G Gaming are required to familiarise themselves with this policy, to adhere to it, and comply with its requirements. This holds true also for those employees not engaged in building G's systems but in using them and interacting with customer data.
- A full consideration of the potential risks from suppliers and third parties are included in our policies and processes. We also require those supplying us and our operators and aggregators to undergo a due

diligence process. However, the details of their own ISMS systems in as much as they do not directly affect G's processes and ISMS, are not part of the scope of this ISO27001.

- *This policy is supported by the Board, and they are responsible for supporting the goals and principles of information security and business continuity in line with the business strategy and objectives.*
 - ISMS policy forms part of G Gaming's induction process. As part of an ongoing programme of Information Security awareness and training, updates are also provided to members of staff.

Related information

Employees are responsible for ensuring that they work in accordance with this ISMS, which follows recognised best practice for Information Security Management and they adhere to the [Code of Conduct](#) which forms part of this environment too. All staff are employed and vetted to meet the requirements of their roles and this is all outlined in our approach to human resource security in line with Annex A7.

Valuable information including personal data is dealt with in accordance with the requirements of Data Protection Act, GDPR, the ISO 27001: 2013 standard and other [applicable legislation outlined in \(A.18.1.1\)](#) with all necessary controls in place as described throughout the ISMS and in particular in [\(A.13.2.4\)](#) for confidentiality agreements with other parties as well as [\(A.15.1.1\)](#) for our supply chain work.

We have a number of partners, associates and suppliers that impact delivery of the services and these are dealt with as part of the Annex [\(A.15\)](#) which has been expanded from purely supplier relationships in the ISO 27001: 2013 standard to include other important relationships too.

Relevant directors and senior management own and review information security policy as part of a Management Review Board and in accordance with the ISMS described in the management requirements and in accordance with our objectives outlined in [\(6\)](#).

Documents

 [IAF_MD17_Issue_2_18042019.pdf](#) Added: 30/11/2022 Added by: [Helen Walton](#) Version: 1.0

Linked work

No Links to display.

4.4: Establish, implement and maintain an ISMS

The organisation shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of ISO 27001 2013

Assigned to: Jakub Szerszen

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 12:54

Categories:

No Categories to display

Added by Cheryl Jones on 25/10/2021 at 14:20

What we do

This completed ISMS.online environment is made up of the following core components for operating, maintaining and improving the organisation's ISMS:

- [This Policies and Controls area](#) and Statement of Applicability
- [The Risk & Treatment area](#)
- [The Interested Parties map](#)
- [The register of Applicable Legislation](#)
- [The Asset Inventory](#)
- [The Management Review Board](#)
- [The Audit Programme](#)
- [The Corrective Actions and Improvements track](#)
- [The Security Incident Management track](#)
- [The Staff communications area](#)

Each area is reviewed and updated in line with [A.5.1.2: Review of the policies for information security](#) and [A.18.2 Information security reviews](#). improvements are managed in line with [10 Improvement](#).

An audit trail of all changes is clearly visible in each area and the Linked Work tool is used to show relationships between individual parts of the ISMS.

This ISMS is designed and developed to allow us to create, collaborate, control and communicate in line with the clause and control requirements. Automatically giving us a contribution towards:

Clauses

- 5.3: Organisation roles, responsibilities and authorities
- 6.1.3: Statement of Applicability
- 7.1: Resources
- 7.2: Competence
- 7.3: Awareness
- 7.4: Communication
- 7.5: Documented information
- 8: Operation
- 9.1: Monitoring & review
- 10.2: Continuous improvement

Controls

- A.5.1.1: Policies for info security approved by management, published and communicated

- A.5.1.2: Review of policies – review at planned intervals, or significant changes
- A.6.1.1: Roles & responsibilities
- A.6.1.2: Segregation of duties
- A.7.2.2: Awareness, education & training
- A.18.2: Independent and technical review of info sec at planned intervals

Linked work

No Links to display.

5 Leadership

5.1: Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 12:57

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 20:39

What we do

We demonstrate leadership and commitment with respect to the ISMS by:

A) Ensuring that the ISMS and IS objectives are established and compatible with the strategic direction of the company - the [Management ReviewBoard](#) includes the most senior executives from the organisation.

In addition workshops have been held with staff where the outputs of these exercises have informed the [internal and external issues work](#) as well as [interested parties](#) and [risk identification](#).

B) Ensuring the integration of the ISMS into the organisation's processes. This environment sets out the processes and controls we use for getting our work done and the staff operate to those processes in practice. Our ISMS is fully integrated into the way we work, it is not a bolt on thing staff need to remember to do, it is our way of working.

C) Ensuring resources for the ISMS are available. As we have embedded ISMS at the heart of the organisation from the top, each member of senior staff has a role to play in their department's area of expertise as set out in [\(5.3\)](#) of the requirements alongside the formal IS specific roles as outlined in [\(A.6.1.1\)](#).

D) Communicating the importance of the ISMS and conforming to it is done as expressed in the requirements 7 and also through (A.7.2.2) of the controls which are reinforced through our [code of conduct](#) and the [staff training materials](#) as well as our internal messaging tools (Notion and Slack).

E) Ensuring the ISMS achieves its intended outcomes is demonstrated through the commitment of the leadership with our [Management Review Board](#) and the fact that the senior management team has all been instrumental in the creation and implementation of the ISMS itself.

F) and G) Directing and supporting persons to contribute to the effectiveness of the ISMS, and continual improvement is demonstrated by the CEO and senior team investment of their own time towards continual improvement as well as every staff member having a role in its effectiveness which is reinforced using the same mechanisms in D) above plus a set of values where continual improvement is essential in a business like ours that is regularly changing and growing to adapt to the [internal and external issues](#) and the requirements of the [interested parties](#) and [risk identification](#). Other areas such as our approach to [audits](#) and [continuous improvement](#) alongside complying with Annex (A.16) for Security Incident Management highlight a commitment to the ISMS.

H) Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. As our organisation continues to grow other individuals will be given the opportunity to take leadership roles in specific areas.

Linked work

No Links to display.

5.2: Information security policy

Top management shall establish an information security policy that meets the requirements

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 18/01/2024

Status: Completed

Approved by Helen Walton on 07/05/2024 13:02

Categories:

No Categories to display

Added by Helen Walton on 18/01/2023 at 12:16

What we do

The organisational Information Security Policy is available as documented information below and can be shared with interested parties as necessary.

All subordinate policies and controls adhere to this policy and are contained within this online ISMS environment and can be made available as specific documents where required.

The Information Security Policies that are appropriate to the organisation can be found within (A.5.1.1) and then considered throughout this ISMS environment illustrating the detailed controls and processes in place. The

Confidential

complementary security objectives are expressed within (6.2) of the standard requirements.

The policies within this specific ISMS environment and overarching system linked to this environment demonstrate a commitment to satisfy the applicable requirements and continual improvement of the management system.

The Information Security Policy needs to work, not only within the ISO27001 standards, but also the individual jurisdictional regulations for ISMS outlined in our [Applicable Legislation](#) Register. In some cases this may require additional audits and policies that are certified by a third party testing house.

Documents

 [Information_Security_Policy_G.docx](#) Added: 07/05/2024 Added by: [Helen Walton](#) Version: 2.0

Linked work

No Links to display.

5.3: Roles and Responsibilities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 30/11/2023

Status: Completed

Approved by Helen Walton on 07/05/2024 13:15

Categories:

No Categories to display

Added by Helen Walton on 07/05/2024 at 13:15

What we do

Dan Rough is the CTO and is the person responsible at a leadership level for ensuring the ISMS conforms to the requirements of the standard as well as carrying out key checks where only the highest level of access is permitted (such as event logs).

Jakub Szerszen acts as an Information Security Manager and Compliance Officer in part of his role as Operations Manager and reports on the performance of the system into the Management Review Board and administering the ISMS.

Dan Rough is the designated Data Protection Officer and leads on aspects relating to the protection of privacy and personal data including personally identifiable information (PII) in compliance with the GDPR, GDPR and the following relevant controls and tools:

These individuals are supplemented by:

Compliance Officer - this individual has overall responsibility for insuring G is fulfilling its overall Compliance responsibilities, this is important because ISMS controls are a crucial part of the licences for suppliers in the UK, the Netherlands, Denmark, Sweden, Malta and other jurisdictions in which G operates.

The Chief Commercial Officer, Helen Walton, who acts as an alternative representative at Board level for the ISMS and Compliance policies.

The Internal Auditor - Natasha Mockett who has overall responsibility for the Internal Audit process, but is supported by the two other Auditors trained by her to assist in auditing the ISMS

- (A.18.1.1) - Identification of applicable legislation;
- (A.18.1.4) - Privacy and protection of personally identifiable information; and
- Legislative risk register.

In addition, members of the [Management Review Board](#) are also responsible for measurement, monitoring, reporting and decision making in accordance with (9.3)

Management Review Board members are risk owners and this is addressed within (6.1)

Each control and policy area within this environment has an owner who is responsible for its updating and reporting into the Management Review Board for any proposed changes or amendments. Authorised staff will have direct team membership of this policies & controls environment.

Any amendments to the ISMS requirements, policies and controls may be applied dynamically, i.e. as the situation requires. For more fundamental changes, after discussion and agreement with one or more relevant Management Review Board members (who in any event independently approve any policy change or are delegating approval in accordance with the roles above). Version control allows us to see who has reviewed and made changes to each policy and thus takes ownership for that review period to present any changes to the Management Review Board.

Where communication is required into staff and other representatives who have access to the ISMS it is done on the relevant Notion page (communication repository used at G) and an alert is put out via our shared communication tool, Slack.

Note that these general responsibilities and role description are complemented by the more specific ISMS requirements described in our [A.6.1.2 Segregation of Duties](#). All staff have a responsibility to read the ISMS, all updates from the Management Board and to follow it in their day-to-day jobs. Staff have a responsibility to look out for and report any breach of the ISMS or external controls (such as the LCCP, GDPR or Anti-Money Laundering) to the Management Board as well.

Responsibilities of each department

Team / Division	Responsibilities	Access Level
Board members	Determine the company's vision and mission to guide and set the pace for its current operations and future development. Determine the values to be promoted throughout the company. Determine and review company goals. Determine company policies. Review and evaluate present and future opportunities, threats and risks in the external environment; and current and future strengths, weaknesses and risks relating to the company. Determine strategic options, select those to be pursued, and decide the means to implement and support them.	

	Determine the business strategies and plans that underpin the corporate strategy. Ensure that the company's organisational structure and capability are appropriate for implementing the chosen strategies Determine the company's appetite for risk and to engage in the process of backing a robust risk management programme focused in the company's business and the area(s) of its activities. Delegate authority to management, and monitor and evaluate the implementation of policies, strategies and business plans. Determine monitoring criteria to be used by the board. Ensure that internal controls are effective. Communicate with senior management.		
Chief Technology Officer	Oversee the development and dissemination of technology Align technological strategies with company goals Build data protection and quality assurance processes Present the technology strategy to investors and partners Communicate with the senior stakeholders Check the audit logs (at highest level of security)		
Data Protection Officer	Responsible for monitoring our compliance with GDPR. Running any necessary Data Protection Impact Assessment (DPIA) Cooperating with or reporting to the Supervisory Authority where this may be required Ensuring G has an appropriate risk-based approach. Making sure we keep and maintain necessary records appropriately.		
Chief Compliance Officer	Oversee the company's overall compliance matters - but with particular focus on gaming regulations Analyse and interpret the relevant rules for entering new jurisdictions Oversee the selection and management of third party test houses Responsibility for having games, RNG and RGS certified and certifications renewed as necessary Stay abreast of regulatory trends and changes to enable the company to react quickly to any new rules. Follow the LCCP guidelines and communicate them clearly to other members Input into game design discussions to ensure responsible gaming is 'baked in'		
Chief Financial Officer	Oversee the organisation's financial activities Analyze the company's financial position Financial reporting on regulatory and management Revenue and expenses control Review and set financial strategy Review and set the company's anti-money laundering policies. Follow up and update all the compliance requirements for the business Review and set the company's structure strategy Act as the company's secretary Communicate with the senior stakeholders Overall responsibility for checking Asset Register, Risk Register		

	and reporting on Incident Management to regulators Oversee Internal Audit process	
Information Security Manager	Manage the ISMS process for the company (reporting to the CTO) Ensure regular running of the Management Review Board, set the timetable for audits and coordinate with external auditors Ensure reminders and staff communications are regular and that any changes to the ISMS are shared with relevant partners Ensure reminders for all ISO27001 components are reviewed within the relevant timetable Liaise with the responsible people to ensure policy compliance on a regular basis (for example that those hiring and dealing with staff leaving are following the processes)	
DevOps engineers	Build and set up new development tools and infrastructure Ensure that systems are safe and secure against cybersecurity threats Identify technical problems and develop software updates and 'fixes' Work with software developers and software engineers to ensure that development follows established processes and works as intended Ensure that disruption to customers and players are minimised during any maintenance, set up or fixes.	
Developers	Design, develop and deliver games accordingly to the vision and strategy defined by the board Perform code reviews to ensure code quality Refactor code to improve the design of existing code Quality test coding in a systematic and thorough way to find problems or bugs and record precisely where the problem was discovered Debug programs and solve complex technical problems that occur within the game's production Maintain and disseminate the highest standards of code quality and technical security as role models to other employees	
Artists (includes Tech Artists and Musicians)	Produce the audio features of the game, such as character voices, music and sound effects Develop designs or initial concepts designs for games including game play Produce the marketing materials Be aware of the potential for security leaks when using local hardware Be aware of risks around IP and trademarks whether of other people or G's own	
Sales & Account Management	Promote the company's vision and introducing new products to the markets and existing customers Research and develop marketing opportunities and plans Research and develop market trends Research new markets and acquire new Customers Execute accounts	

	Stay current in the industry by attending conferences and workshops Act as the voice of the customer within product development to ensure games and systems are fit for purpose Be vigilant regarding risks to customer and player data Be aware of the impact of GDPR and relevant legislation on customer communications via the website etc Be aware of the LCCP and relevant regulation relating to marketing, advertising and game description in the real-money gaming industry.	
Producers (includes Game Designers and Mathematicians)	Plan what works needs to be done to accomplish the project Look at the risks involved in a particular project and manage these risks Coordinate and liaise with multiplier stakeholders including customers and third party testing bodies Oversee and manage the projects Ensure the product development and design occurs with an awareness of potential ISMS risks and conforms to best practice internally Ensure testing of products takes account not only of regulatory requirements, but also of ISMS best practice Stay up to date with the latest changes and requirements to product design within the real money gaming industry - particularly as far as regulatory requirements apply.	

Linked work

No Links to display.

6 Planning

6.1: Risk assessment process

A documented information security risk assessment process, and the treatment thereafter in accordance with that process

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 26/04/2024

Status: Completed

Approved by Helen Walton on 07/05/2024 13:22

Categories:

No Categories to display

Added by Helen Walton on 18/01/2023 at 12:21

What we do

A comprehensive yet pragmatic approach to risk identification, analysis and treatment as well as ongoing monitoring and review is set out in the attached policy methodology document. It addresses risks arising from internal and external issues, whether threat or opportunity based and outlines the approach to risks arising from [A18.1.1 Applicable Legislation](#).

The [risks & treatments](#) tool is used to analyse risks identified from the analysis. We record these in our risk register. Specific areas that need larger discussion - for example changes recommended following an incident - may have procedures outlined and refined in our internal wiki, Notion, before being summarised in the risk register.

A monthly risk meeting has been added to the Directors calendars to discuss operational risk. Any changes to longer term risks are then added to the Risk Treatment Plan.

Documents



[Risk_Analysis.docx](#) Added: 07/05/2024 Added by: [Helen Walton](#) Version: 2.0

Linked work

No Links to display.

6.1.3: Statement of Applicability

Produce a Statement of Applicability that contains the necessary controls and justifications for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A.

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 13:22

Categories:

No Categories to display

Added by ISMS Creator on 22/10/2021 at 09:01

Statement of Applicability report

The version 1.0 of the Statement of Applicability (SOA) is available [here](#) and can also easily be found from the headlines tab and structure tab. The SOA report addresses each Annex A control and its applicability with relevant justifications. It provides an online report facilitating quick links and overview to the more detailed parts of the ISMS and offers a simple export report option.

The SOA is dynamically updated as Annex A policy/control changes and updates occur in their respective activity areas which are linked. Further detail can be found on the controls in use e.g. the actual policies behind

them and any risks being addressed by the controls.

Risks associated with the SOA are included in the [risk treatment plan](#) in line with [\(6.1\)](#) and [\(A.6.1.2\)](#) then referenced back where appropriate to the applicable Annex A controls.

Any earlier versions or material changes that need to be exported and held for audit purposes can be uploaded into this environment and the version control process used to manage that history.

Linked work

No Links to display.

6.2: Information security objectives

Establish applicable (and if practicable, measurable) information security objectives, taking into account the information security requirements, results from risk assessment and treatment. Determine what will be done, what resources are required, who will be responsible, when they will be completed and how results will be evaluated.

Assigned to: Helen Walton
Days estimated: 0.0
Days taken: not set
Due: not set
Status: Completed
Approved by Helen Walton on 07/05/2024 13:23
Categories:
No Categories to display
Added by Helen Walton on 21/04/2023 at 11:37

What we do

The information security objectives described below have been established after taking into account:

- The context, purpose and internal as well as external issues affecting the organisation [\(4.1\)](#)
- Determining the requirements of the interested parties [\(4.2\)](#)
- The boundaries of the ISMS [\(4.3\)](#)
- The risk assessment and treatment [\(6.1\)](#)

Objectives and measures:

The objectives, measures and frequencies for measurement we have chosen below are business led, pragmatic and aim to deliver on one or more of the standards we have chosen to apply. The table below sets out the headline information:

ISO Standard	Objective	Measure	Target	Frequency	Owner	Source and Evidence
--------------	-----------	---------	--------	-----------	-------	---------------------

ISO 27001:2013/17	Game service availability	% uptime of the service	99.5%	Monthly	CTO	website analytics (summarised into uptime KPI in Management Board Reviews)
ISO 27001:2013/9	Access and Data integrity	unauthorised access	0	monthly	CTO	System Logs
ISO 27001:2013/12	RTP Monitoring	within expected tolerances depending on volatility	+/- 5%	Monthly	CTO	Periscope Data
ISO 27001:2013/15	Customer Service Response	time to response, successful closures	as per SLA	Daily	AMs	Daily Standup, Freshservice

Other than contractual obligations in (A.13.2.4) for relevant delivery into customers, the [Management Review Board](#) sets the objectives and targets for each of the measures.

Performance is documented within the Management Review Board reporting and management area, using KPIs where appropriate, Track statistics and other reports from operational systems and other reports as required. These objectives and their measures with performance results are evaluated at management reviews as part of 9.3 or by exception in between those periods if an incident or something else causes an adverse impact on targets or normal performance expectations.

Where appropriate, results and decisions will be communicated out to staff and other interested parties using the normal channels for communication of any specific work, and the team awareness & communications group for overall information. All measures are owned by a member of the Management Review Board and source data may be delegated to relevant members of staff to obtain and share as needed. Actions, tasks and any resultant work falling out of the evaluation is either documented in the Management Review Board area as part of that review, or specifically documented inside the appropriate operations environment e.g. order management, website, CRM system.

Linked work

No Links to display.

7 Support

7.1 - 7.4: Resources

The organisation shall determine and provide resource for the establishment, implementation, maintenance and continual improvement of the information security management system. The resources affecting its performance shall be competent and aware, enabled by relevant internal and external communications.

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 30/11/2023

Status: Open

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 16:19

What we do

The organisation has determined the resources, competences, awareness and communications capabilities necessary for establishing, implementing and maintaining as well as continually improving the management system. This is evidenced by:

- Leadership resource commitment expressed in [\(5.1\)](#) and [\(9.3\)](#)
- Providing the resources for the ISMS per [\(A.6.1.1\)](#)
- Activity owners and supporting team members for each one of the requirements, policies and controls for the standards we have chosen to apply.
- Creation of this ISMS.online environment for overall policy control and the enabling infrastructure to deliver work such as [ISMS Management Review Board reviews per \(9.3\)](#), [Internal Audits per 9.2](#), [Nonconformities and Corrective Actions per \(10.1\)](#) and [Risk Assessment & Treatment per \(6.1\)](#)
- Specific resources allocated for risk management [\(6.1\)](#), [internal audits \(9.2\)](#), [nonconformities](#), [corrective actions](#), performance evaluation and ongoing improvement and specialist areas of work such as managing information security incidents.
- Mechanisms for efficiently communicating and engaging all staff and supply chain resources in the scope of the management system such as our Notion pages.
- Use of our Onboarding process to ensure staff understanding and compliance of the policies underpinning their role performance.
- Communicating externally with particular emphasis on how employees [communicate with authorities \(A.6.1.3\)](#), how they might need to use a whistle-blowing policy, and to be aware of particular confidentiality issues with customers or competitors (Code of Conduct) and sensitivities with the public or media (Social Media Policy).
- Resource investment in the ISMS.online management system platform for the professional implementation and ongoing delivery of the management system to ensure that our limited physical resources are optimised and focused

Our resources involved in the establishment, implementation, maintenance and continual improvement in the management system are senior experienced staff, experts in their fields. They have all read around the subject matter for each standard, hold certifications where appropriate and recognise the importance of staying up to date with developments in their respective fields as regards improvements. This includes training and development as required, both informally e.g. online personal development, and formal training programmes with certification at the end.

Harnessing best practice tools such as ISMS.online with built-in competence for related areas e.g. risk assessment and supplier management are also evidenced throughout the management system.

The organisation's culture and values push us towards continual improvement. Information security is a thread like commercial development or organisation change that we constantly work on in our day jobs. This is also evidenced where we take the opportunity to further improve practices by following up research from staff, staying abreast of what works in the firm and elsewhere.

Linked work

No Links to display.

7.5: Documented information

The information security management system shall include documented information required by the ISO 27001 and other information determined by the organisation as being necessary for the effectiveness of the system. Creation and updating will include ID and description, format and media along with review and approval, and history of changes. It must be available and suitable for use when and where needed and adequately protected from loss of confidentiality, improper use or loss of integrity.

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 13:30

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 21:53

What we do

7.5.1 General

This ISMS includes:

- a) documented information required by the International Standard as set out in this ISMS workspace and its linked initiative areas that make up the complete ISMS.
- b) documented information deemed necessary by the leadership for the effectiveness of the ISMS.

Our approach takes into account the organisation size, appetite for risk, complexity of our business, desire for digital/paperless working, and the competence as well as capacity of the people within the organisation.

Our approach to the documented information is pragmatic, focused on pithy communication to get the work done and appropriately auditable for both a) and b) above.

7.5.2 Creating and Updating

For creating and updating:

- Reference numbers of the ISMS follow the ISO 27001 and 27002 nomenclature and taxonomy with appropriate titles with all the detail held in activity areas like this one, aggregated by relevant deliverables and phases elegantly presenting a specific area of the standard.
- Owners, authors and time stamps of work published are captured by the user details logged and presented in the relevant activity interface.
- Activity notes areas are to be used for all controls and policies documentation unless the policy or control is of a complex or lengthy nature, when documents can then be uploaded into the relevant activity area and controlled as outlined below.

Notes version control is done automatically with the history of updates and changes available on the page. No version number is required per se, it is logged by author, time and in chronological order digitally on the platform.

The following standards for version control of documents are used (not least because they can become uncontrolled when shared with others or misalignment on versions is more likely):

- Ver 0.1 and increments thereafter signifies draft to self and not normally shared
- Ver 1.0 onwards signifies first published document to the target audience
- Ver 1.1 onwards signifies minor changes to the published document
- Ver 2.0 onwards signifies a major release to the published audience

And the cycle continues thereafter up to a maximum of 99.99 in line with the online document management system standards within this platform

ISMS Document Specifics:

- Document name: the name of the document shall be clear and ideally be uploaded to the control activity where it is being applied. It shall also include the version number per above.
-
- Document owner, issuer, issue (version), date of issue and change control are all to be pragmatically captured and any changes or detail can be summarised on the platform in notes, discussions or within the document upload description.
- Documents sometimes originate outside the organisation but which need to be protected or controlled as part of the ISMS or our contractual obligations with customers, partners and others. These are incorporated into our document classification, version control and management requirements by means of overmarking or revising if appropriate, or by simply adding into the relevant third party account area as that overrides all document markings by being deemed a Commercial in Confidence environment.

Information classification is described in more detail [per \(A.8.2.1\)](#).

- The format of the ISMS is written in English, digitally presented in the online system with text notes and where appropriate complemented by documents and specialist tools e.g. risk assessment and treatment tool. Other than a visitor book control which is paper-based, and physical infrastructure management e.g. office locks all other controls and policies are digital as expressed in this environment and evidence of compliance is held in the relevant technology system.
- Review and approval of controls for suitability and adequacy is governed by having a different Management Review Board member approve the work of others. This is evidenced in the relevant activity area to demonstrate that the person completing the activity and submitting it for approval is different to the person approving it. NOTE: the only area we allow to be approved by the same person as the one

submitting it is the asset register maintenance in [\(A.8.1.1\)](#) due to the frequent changes or updates to assets.

7.5.3 Control of documented information

- a) By having all the ISMS documented information in the online platform, it is just a click away from a user's normal day to day work and also controlled in more detail throughout the ISMS environment.
- Using the online platform means the ISMS is easily accessible for staff and others* who have the correct permissions to access it.
- b) It is adequately protected from:
 - Loss of confidentiality - the platform has unique permission and privacy system that prevents unauthorised users gaining access to the private areas of the ISMS. Using the principle of team memberships, an Management Review Board member will need to grant access to a user of the platform for them to see the ISMS and only Management Review Board members or their nominated users can update the system (effectively by having admin and management rights to the online system area).
 - Loss of integrity - given the discreet permissions applied to team members once they are visible there are controls on what users can do to change the system e.g. once an area is locked down it cannot be changed unless reopened by an authorised user. Users can still view and access the information. Full audit controls and database record logging also highlight any changes that have been made whether supportive (or sabotaging.)
 - Loss of availability - per [\(A.12.3.1\)](#) information backup services preserve and protect any loss of availability and being a cloud-based service it can be available more readily to the relevant users wherever they are.
- c) to e) is as described above for distribution, retrieval, access and use including control of changes
- f) when a change is required to the documented information (whether from a management review, security incident or general improvement observation), the locked control or policy activity area is reopened by a Management Review Board member or authorised manager/administrator. It is then updated as required with the audit of changes to the notes saved as records, and earlier versions of documents held in the relevant version control area of the activity. No deletion is carried out of earlier records at that stage (unless a genuine mistake has occurred e.g. document uploaded in the wrong area). The overall retention and disposition of documented information is dealt with as per the policies on retention and disposal of information in [\(A.8.3.2\)](#). and [\(A.18.1.3\)](#)

*Those who can access the documented information held in the ISMS within this policies and controls environment include:

- Management Review Board members who have direct access to the project environment
- Staff, by means of their membership of the [Staff Communications](#) or via a Policy Pack access
- Relevant outsourced associates/suppliers ([per A.15.1.1](#)) by means of their relevant [Staff Communications](#) membership or via a Policy Pack access
- Temporary membership for accreditors and auditors
- Temporary membership for customer and prospect Information Assurance representatives

Other memberships for areas of the ISMS that include security incident management, internal audits, management reviews, nonconformities and corrective actions are also controlled by team memberships. Unless otherwise agreed by a Management Review Board member, access to these initiative areas are limited to Management Review Board members and staff specifically engaged in relevant work.

Retention of records

Our policies around the retention of records are described in [\(A.18.1.3\): Protection of records](#)

Linked work

No Links to display.

8 Operation

8.1 - 8.3: Planning and control

Plan, implement and control the processes needed to meet information security requirements and achieve the information security objectives including planned risk assessments and treatments.

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 30/11/2023

Status: Completed

Approved by Helen Walton on 07/05/2024 13:31

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 21:55

What we do

In meeting the requirements for 8.1 around operational planning and control, we plan, implement and control the processes to meet information security requirements and implement actions as determined by [\(6.1\)](#), and in accordance with the objectives noted in [\(6.2\)](#). This whole environment with all the policies and controls also exhibits our approach to planning and control, with [\(9.3\)](#) illustrating how we manage that as part of regular management reviews.

Our approach for documented information beyond [\(6.1\)](#) and this environment is presented in [\(7.5\)](#).

In meeting the requirements for 8.2 and 8.3 we perform risk assessments in accordance with the policy outlined in [\(6.1\)](#), and use the tools linked to that environment such as [risk assessment and treatment](#) as well as [applicable legislation risk](#) tools. All of the work done enables retention of the documented information within the tools and offers links back to the controls and policies used to address the risks and issues.

Linked work

No Links to display.

9 Performance evaluation

9.1: Performance evaluation

Evaluation of the information security performance and effectiveness of the system. Includes what should be monitored, the measurement, analysis and evaluation, when and who does it, and who analyses and evaluates the results

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 13:33

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 21:57

What we do

The organisation has decided what to monitor and measure following its planning and research work in [\(4.1\)](#), [\(4.2\)](#), [\(4.3\)](#) and subsequent risk analysis in [\(6.1\)](#).

[\(6.2\)](#) then sets out the business objectives for the ISMS and that activity area includes what will be monitored, measured, who does it, when and how that is sourced and evidenced.

Evaluation of the ISMS is done regularly through management reviews in line with [\(9.3\)](#) by the Management Review Board and through internal audits in [\(9.2\)](#).

In the event of any nonconformity, corrective action, improvement or incident arising that is then dealt with in line with clause [\(10\)](#). All of this is managed inside the ISMS.online platform and enables a holistic approach to monitoring, measurement and evaluation to ensure objectives are achieved and continuous improvement for the organisation and its interested parties.

Applicable legislation and compliance obligations are addressed within [\(A.18.1.1\)](#).

Linked work

No Links to display.

9.2: Internal audits

Internal audits to be conducted at planned intervals to provide information on whether the system conforms to the requirements and is effectively implemented and maintained. Demonstrate a plan for the audit programme, with the criteria and scope, selection of auditors, reporting to relevant management and that evidence of the programme and results are retained.

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 15/11/2024

Status: Completed

Approved by Helen Walton on 07/05/2024 13:34

Categories:

No Categories to display

Added by Helen Walton on 30/11/2022 at 21:25

What we do

We conduct internal audits at planned intervals to determine whether the control objectives, controls, processes and procedures of the ISMS:

- Confirm compliance to the requirements of the ISO standards and related certifications we hold as well as meeting regulatory requirements e.g. for GDPR
- Meet the expressed information security requirements and perform as expected
- Open up opportunities for further improvement individually and or collectively
- Enable feedback for the auditees on their own performance

Internal Audits are planned by the Management Review Board and delivered through an [Audit Programme](#) within the online platform which demonstrates our programme for at least 12 months ahead.

In summary the audit programme addresses:

1. Conducting two audits prior to certification (to prove consistency of process):
 - a. A whole ISMS documentation review prior to Certification Stage 1 audit.
 - b. A second, pre-Stage 2 audit of a process or focus area(s).
2. A three-year audit cycle that covers the entire ISMS. The standard requires, at a minimum, full coverage of the ISMS in the three-year certification period. This is a controls-based programme with the standard divided into five audits. A sixth audit to cover a specific process or number of focus areas rounds out the programme.
3. Audits focused specifically on the areas associated with Personal Data as required for GDPR/DPA 2018 to meet the ICO data protection assessment compliance in line with our GDPR compliance work.

In addition to the internal audit programme, it also sets out the external audits for surveillance and recertification.

Alongside the audit plan, and the ongoing risk assessment outlined in [\(6.1\)](#), we also review each policy and control at least annually to ensure it remains fit for the purpose. This is described in more detail in [\(A.5.1.2\) review of policies](#).

Guidance for undertaking audits:

There is no formal requirement for a policy on completing internal audits however we have taken the opportunity of outlining our internal guidance on the approach towards audits and related policy reviews below.

All audit work is focused on quality, not quantity, and simple pithy communication not verbose reports or bureaucracy for the sake of it. The goal of an audit is to identify nonconformity and or areas for improvement, as well as highlight areas of good practice that can be spread elsewhere.

Process

This process will be followed for:

- The main audit programme both pre-certification and post-certification
- Where simple policy reviews identify a need for a more significant additional audit
- Risk assessments suggest an additional audit is worthwhile
- The Management Review Board decide to focus attention on improving one or more parts of the ISMS given the importance of the processes concerned

Audits are usually assigned to either specialist advisers, senior management or internal staff not directly involved in the day to day work, who can offer objectivity. Our Internal Auditor has undertaken independent, certified training and has in turn trained two other staff as Internal Auditors. The notes on this training and our process are [held in Notion](#)

On occasions, for either sensitivity reasons or resource constraints, there may be senior staff who are involved as part of the day job too; in these instances objectivity is assured through independent evaluation of the findings/recommendations and further investigation if required as determined by the Management Review Board.

The code of conduct reinforces that all staff are expected to deliver the work with values that demonstrate a desire for continual improvement and in accordance with their employment terms.

Any detailed terms of reference for each audit are determined by the Management Review Board prior to the audit activity and these shall include:

1. Scope of audit (i.e. ISMS areas to be audited)
2. Method of audit (e.g. remote/on-site, observation, interview, analysis of records)
3. Selected auditor(s) - to ensure objectivity
4. Controls to be audited within the ISO 27001 ISMS and any related compliance regimes
5. Any nonconformities and corrective actions are retained as documented information within the relevant audit activity and when required managed for change in the [Corrective Action and improvement Track](#).
6. Any nonconformities and corrective actions need to be addressed based on their risk impact in accordance with the process outlined in clause [\(10.1\)](#).

Evidence and content expectations

Findings, both positive and negative will be documented at a high-level in the relevant column of Scope and Detailed Findings table in the audit activity area.

Any identified nonconformities or opportunities for improvement will be documented in a simple fashion in that column of the table and link to the specific item raised within the [Corrective Action and improvement Track](#) in accordance with [\(10.1\)](#).

A link between the audit activity and the item in the track will also be created in the "Linked Work" section to further improve linking of audit findings to corrective actions and improvements.

If appropriate, the results of the audits are presented to the auditees in the first instance by the auditor and any discrepancies addressed by both the auditee and auditor as required, including comments captured about how to improve nonconformances or reinforce positive practices.

Disputes in findings are to be raised within the report /activity and resolved by the Management Review Board.

Staff are engaged and made aware of any changes following audits in the normal manner, either through the [Staff Communications](#) group, or if of a more personal nature then in their personal HR area.

The results are then reviewed by the Management Review Board either at the regular board meetings as part of the requirements within [\(9.3\)](#), or earlier if high risk impact nonconformances are presented, that if left unaddressed, expose unacceptable vulnerabilities to the organisation, its customers or other [interested parties](#).

Linked work

Projects

Audit Programme	Progress	34%
-----------------	----------	-----

Risks

A: Information systems and practices fall out of compliance with the organisations information security policies and standards	Risk map: Risks & Treatments	19 Overdue
	Project: ISO 27001 Policies & Controls 2022	

9.3: Management review

Top management review of the information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness, using an agenda that considers the requirements of 9.3.

Assigned to: Helen Walton
Days estimated: 0.0
Days taken: not set
Due: 30/11/2023
Status: Completed
Approved by Helen Walton on 07/05/2024 13:36

Categories:
No Categories to display
Added by Helen Walton on 04/03/2022 at 22:24

What we do

We operate a special board called the [Management Review Board](#) which sits at planned intervals to ensure the management system and its objectives continue to remain suitable, adequate and effective given the

Confidential

organisation's purpose, issues and risks, previously addressed within (4.1), (4.2) and (6.1).

The Management Review Board has a private workspace project area which enables the members of the board to collaborate and work well together on the items in scope for the management review. The meeting intervals are documented in that area and generally planned annually in advance with a target frequency of bi monthly going to quarterly as a minimum.

Representatives on the board are added as team members in the private area and selected in line with

- (5.1) Leadership and commitment
- (5.3) Organisational roles, responsibilities and authorities
- (A.6.1.1) Information security roles and responsibilities

Collaboration, information sharing generally, preparation for reviews, related work around management review topics are conducted on a dynamic basis, and documented in the online platform as well as following a standard agenda for formal reviews. Meetings will be held remotely but all follow the same agenda.

The agenda for Management Reviews is a standard format each period following expectations laid out by ISO. It includes consideration of:

- a) The status of actions from previous management reviews;
- b) Changes in external and internal issues that are relevant to the management system;
- c) Feedback on the performance, including trends in:
 - 1) nonconformities and corrective actions;
 - 2) monitoring and measurement results (including security incidents);
 - 3) audit results; and
 - 4) fulfilment of objectives;
- d) Feedback and other relevant communications from interested parties;
- e) Results of risk assessment and status of risk treatment plan; and
- f) Opportunities for continual improvement or any other changes required to the management system.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the management system.

The Agenda above is followed for each Management Review.

Each review is then simply documented as evidence to meet the requirements. Where the ISMS.online environment provides reports and insight automatically e.g. with incident statistics, or risk assessment then that will simply be linked to rather than duplicated.

Actions arising from that review will then be managed in the review area e.g. a task for further investigation, or the work taken into its specific workspace e.g. a nonconformity set of actions will continue to be managed from the non conformity track item. This makes it very quick and easy to see actions from previous reviews and run reviews efficiently. Reviews from the previous period get closed off (activity marked as completed) at the start of the following review, once confidence that all previous actions have been completed with that first agenda item.

Linked work

Projects

Management Review Board

Progress

65%

10 Improvement

10.1: Nonconformities and corrective actions

Demonstrate how nonconformities and corrective actions will be addressed

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 30/11/2023

Status: Completed

Approved by Helen Walton on 07/05/2024 13:38

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 22:37

Policy

When a nonconformity occurs, the organisation shall:

A) react to the nonconformity, and as applicable:

- 1) take action to control and correct it; and
- 2) deal with the consequences;

B) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

- 1) reviewing the nonconformity;
- 2) determining the causes of the nonconformity; and
- 3) determining if similar nonconformities exist, or could potentially occur;

C) implement any action needed;

D) review the effectiveness of any corrective action taken; and

E) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organisation retains documented information as evidence of:

- F) the nature of the nonconformities and any subsequent actions taken and
- G) the results of any corrective action.

The documented evidence is retained in the [Corrective Actions and Improvements Track](#).

This nonconformity process is incorporated into a broader improvements process where the primary goal of a Corrective Action following identification of a nonconformity or broader improvement is to fix the problem and ideally address the underlying 'root cause' such that the problem does not occur again.

Corrective Actions and general improvements are brought about through various means, for example:

- Service Request
- Internal Quality Audit
- Customer Complaint / Concern
- Staff Observation
- Trending Data from a KPI or other measure
- Risk Assessment
- Process Performance Monitoring Review

Work in scope for this corrective action process is:

- Nonconformances identified during Internal or External Audits against documented operating controls (not where gaps are identified e.g. from a first audit)
- Business and organisation oriented nonconformance that is not addressed within the normal course of the maturing business growth and change (see below)
- Repeating issues experienced by a range of stakeholders (i.e. not one-off or infrequent issues for one customer)

All corrective action and improvements in scope will be managed and delivered on the [Improvement Track](#). If appropriate, changes will also be made to ISMS policies and controls thereafter with the approval of the Management Review Board during its regular meeting cycle, or by exception if an urgent change is required.

Work out of scope for corrective action management is:

- issues that are infrequent or one off. These should be managed from within the normal support case management system as set out in normal operating procedures.
- minor course corrections or evolutions to business practices that are addressed by line managers with their staff as part of general standards improvement within a growing business

Undertaking Corrective Actions and Improvements

Corrective actions and improvements follow a simple process on the Track with status as follows:

- **To do**
- **Assessment**

- **Awaiting Board approval**
- **Implementation**
- **Monitoring**
- **Resolved**
- **Archived**

This process is described in further detail below, and it is coordinated by an Management Review Board member:

Following identification of a nonconformity or general improvement as described above for work in scope, the 'item' will be placed in the '**To Do**' list of the Track and addressed based on the ongoing impact of the item. In simple terms nonconformities and improvement requirements with a major (high) impact will be dealt with more quickly than (minor) low impact nonconformities, with all being addressed and monitored as part of the Management Review Board reviews in accordance with 9.3.

Major nonconformities are typically items that would mean failure to retain certification of the ISMS if audited there and then, or bring about serious performance issues in the business that are likely to affect multiple customers and or prevent significant growth. All other nonconformities are minor.

Items being worked on will then be moved to the next stage of the Track '**Assessment**'. Work delivered at this stage, depending on its significance, may include:

- Noting the Interested Party/s that work is now underway (if relevant they are kept informed)
- Identifying the problem and explaining the existing situation including if appropriate size & frequency of the nonconformance.
- Acknowledging report source/s and demonstrating or linking to evidence (where necessary)

If the problem just needs remedial action then the appropriate lead team member is assigned to make the change to **Implementation**, and demonstrate the steps being taken to avoid any further adverse effects, bypassing the need for wider Management Review Board consultation and board time. Items that are potentially reputation affecting for multiple clients, have significant costs or resource impacts on change are submitted for approval and decision making either within the Management Review Board, or by exception dynamically if required.

Once Implementation is complete the item is moved to the '**Monitor**' stage of the Track and monitored until such time as the change has been deemed sustainably successful by the Management Review Board - as determined in the regular management reviews.

After that period the item is moved to the '**Resolved**' stage where it becomes business as usual again. All stages are reported on as part of the management review in (9.3). When appropriate items can be moved from the resolved stage to an '**Archived**' position.

If the problem needs further investigation then the **Assessment** process continues with more detailed analysis to ascertain the underlying root cause before remedial action is taken. Work includes:

- Relevant team members and stakeholders invited to participate in a root cause analysis workshop and encouraged to bring data, evidence, information as they see fit.
- Relevant exercises* can be conducted to help identify the underlying causes and the process continues until the root cause is found.
- Once root cause analysis is complete then options for solutions are considered and prioritised based on criteria germane to the problem being solved (e.g. quality, cost, time, impact and whether to deliver

change in stages such as quick wins and longer term changes).

- If the changes require budget and physical resource then the recommendations are presented to the Management Review Board before action is taken (recommendations can be made outside the normal Management Review Board meeting process especially if the nonconformity needs to be addressed before the next Management Review Board meeting, but all nonconformities are still reported on as part of the regular management reviews in (9.3).
- Depending on the magnitude of the change required, the **Implementation** work can be delivered within the Track and evidenced from there, or if a more significant change that needs a bigger team and work breakdown, it may be addressed using a separate project. The work will be connected to the Track for management and audit purposes.
- Once **Implementation** is complete it then moves into the latter processes as described above.

All corrective action work is held on record by the Management Review Board in the Track for audit and learning purposes.

Where required e.g. for an Interested Party, a communication will be made back to the original report source (e.g. external auditor, customer) that the nonconformance has been addressed and where appropriate an invite given to them to evaluate the results of the Corrective Action or general improvement.

*Corrective Action exercises

Corrective Action exercises that can be undertaken by individuals as well as teams to help uncover root cause issues include:

- Brainstorming (clustering ideas, prioritising and selecting the most relevant ones for further analysis)
- 5 'why's (asking 'why' about the problem cause at least 5 times to uncover the root cause)
- Fishbone/Ishikawa diagrams
- Flowcharts
- Benchmarking against other practices to compare / contrast performance
- Control charts & checklists
- Keep, Stop, Start analysis

Linked work

Tracks

Corrective Actions & Improvements

Open: 15 Overdue: 3

10.2: Continual improvement

Demonstrate how the organisation shall continually improve the suitability, adequacy and effectiveness of the information security management system

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 30/11/2023

Status: Completed

Approved by Helen Walton on 07/05/2024 13:38

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 22:38

What we do

The organisation shall continually improve the suitability, adequacy and effectiveness of the ISMS by living the controls, policies and processes expressed within this environment and use of the wider ISMS tools. Specific examples include:

- [Regular management reviews per \(9.3\)](#)
- [Internal Audits per \(9.2\) including ISMS scope and specific policy reviews](#)
- [Corrective Actions per \(10.1\)](#)
- [Ongoing and regular risk assessment based on the risk methodology set out in \(6.1\)](#)
- [Addressing security incidents in line with Annex \(A.16\)](#)
- [External independent audits as required](#)
- [General organisation values and team working as expressed within the day to day culture, and documented as part of the \[code of conduct\]\(#\) and \[employment terms\]\(#\).](#)
- [Ongoing staff engagement from the point of recruitment, through onboarding and engagement in our continuous improvement programme. During exit, where appropriate, staff are also asked about reasons for leaving and opportunities for improvement, and if these relate to the ISMS then they can also be factored into the review process in the normal manner as well.](#)

The documented evidence is retained in the [Corrective Actions and Improvements Track](#) and the respective audit and incident management areas.

Linked work

No Links to display.

A.5. Information Security Policies

A.5.1 Management direction for information security. Objective: To provide management direction and support for information security in accordance with

business requirements and relevant laws and regulations.

A.5.1.1: Policies for information security

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 30/11/2023

Status: Completed

Approved by Helen Walton on 07/05/2024 13:39

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 22:39

What we do

The organisational **Information Security Policy** presents the board-level commitment to information security and over-arching policy statements. This document can be found in [\(5.2\) - Leadership/Policy](#).

Subordinate policies include, but are not limited to:

- [Access Control Policy \(A.9.1.1\)](#)
- [Acceptable Use Policy \(A.8.1.3\)](#)
- [Change Management Policy \(A.12.1.2\)](#)
- [Code of Conduct](#)
- [Cryptographic Controls Policy \(A.10.1.1\)](#)
- [Information Backup Policy \(A.12.3.1\)](#)
- [Information Classification Policy \(A.8.2.1\)](#)
- [Information Security Incident Management Policy \(A.16.1.1\)](#)
- [Information Transfer Policy \(A.13.2.1\)](#)
- [Mobile Device & Teleworking Policy \(A.6.2.1 & 2\)](#)
- [Physical Security Policy \(A.11.1.1\)](#)
- [Secure Disposal & Reuse Policy \(A.8.3.2 & A.11.2.7\)](#)
- [Terms & Conditions of Employment](#)

Policy

The purpose of this policy is to ensure the organisation has a set of information security policies designed to direct the behaviour of individuals in a manner that is adequate and proportionate to associated risks.

Policy Statements

1. The organisational Information Security Policy is the top-level policy below which all other information security policies are subordinate.
2. All subordinate policies must adhere to and support the organisational Information Security Policy.
3. Each policy will have an owner who is responsible for:
 - a. Ensuring the policy is understandable; pragmatic & enforceable; adequate & proportionate; and made available to relevant personnel (who may be external to the organisation).
 - b. Policy review and maintenance in line with [\(A.5.1.2\) Review of the policies for information security](#); and
 - c. The logging and authorisation of policy waivers and exceptions.
4. Policies must be approved by authorised management.
5. Policies will be made available to all relevant personnel.
6. Any policy made available must be read, understood and complied with.
7. Any waivers or exceptions to policies must be authorised by the relevant policy owner, logged and managed.

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.5.1.2: Review of the policies for information security

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 15/11/2024

Status: Completed

Approved by Helen Walton on 07/05/2024 13:39

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 30/11/2022 at 21:23

What we do

Regular review of information security policies is undertaken in line with the policy below.

Evidence of review is logged with policy areas updated with automated time stamps and audit trails in the main policy and controls area.

Policy

The purpose of this policy is to ensure that the organisation's information security policies are reviewed at planned intervals and are maintained against change to ensure their continued suitability, adequacy and effectiveness.

Policy Statements

1. The policy owner is responsible for its review.
2. A policy must be reviewed at least annually but will also be reviewed periodically as part of the 3 year internal Audit Programme.
3. A review must also be conducted whenever significant changes are made that would impact a policy, regardless of the nature of the change (e.g. business change; legislation change; technology change).
4. The review must include assessing opportunities for improvement of the policy.
5. Changes to a policy must be approved by a member of the Management Review Board.

Consequences of noncompliance with this policy

Any noncompliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Process

Policies planned for review have 'To Do's' inside them and are aggregated up to the master 'to do' tabs.

Each policy owner will also receive an email alert when the policy is due for review.

1. To evidence the review, the relevant activity area will be reopened and reviewed.
2. If no change is required it will be resubmitted for new approval and timestamped with the Management Review Board approver details.
3. If the review identifies a small change or recommendation is required it can be done immediately in the policy area and resubmitted for approval by a member of the Management Review Board.
4. If a nonconformity, corrective action or major opportunity for improvement is identified then an item will be raised for action in the [Corrective Actions & Improvement Track](#).
5. Any material changes that require staff awareness and engagement (i.e. that affect their ability to comply with the ISMS policies) will be done in line with organisational communications and compliance channels.

Linked work

No Links to display.

A.6. Organisation of Information Security

A.6.1 Internal organisation. Objective: to establish a management framework to initiate and control implementation and operation of information security within the organisation.

A.6.1.1: Information security roles and responsibilities

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 15:54

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 15:54

What we do

We demonstrate the leadership aims of the standard and allocate roles in accordance with the management requirements of ISO 27001:2013 specifically for [\(5.1\)](#).

We have a Management Review Board that is made up of the senior management team and sits over the ISMS in line with [\(9.3\)](#). Collectively this body takes the main strategic decisions around information security and issues affecting performance and it is chaired by the CISO.

All risks identified from internal and external issues, interested parties requirements and other systems inputs are risk assessed and treated in accordance with [\(6.1\)](#). All ISO 27001: 2013 requirements, policies and controls have a specific owner as illustrated in the relevant activity area (like this one).

All risks, and residual risks also have owners where their accountability is made clear in the relevant tool as the risk owner.

Whilst work can be delegated to other staff in the organisation or indeed other interested parties like suppliers, the risk owner is clear and they ultimately report into the Management Review Board if not also being part of that Board. Completion of delegated tasks and related work is evidenced in the relevant risk tool per the policy in [\(6.1\)](#) or in linked initiatives.

All staff have within their [employment terms and conditions](#), and [code of conduct](#) the reference to information security, the need to follow the information security policy and code of conduct, and other specific job specific procedures as required.

Defined Roles & Responsibilities within the ISMS

Name	Role	Responsibility
Paul Dolman-Darrall	CEO	Top-level ownership of risk within the organisation
Dan Rough	Chief Technology Officer (CTO)	Top-level ownership of the ISMS and information security, including the technical aspects of the ISMS and information security
Jakub Szerszen	Acting Compliance Officer and Information Security Manager	Ensure the integration of jurisdictional Compliance aspects with the overall ISMS
Dan Rough	Data Protection Officer (DPO)	Privacy and data protection relating to personally identifiable information (PII)
Natasha Mockett	Chief Financial Officer (CFO)	Legal & regulatory compliance, overseeing HR. Internal Auditor
Helen Walton	Chief Commercial Officer	Contractual information security obligations
Natalie Millett	Finance	Asset register

Documents

 [organisationalStructure Jan 2024.pptx](#) Added: 07/05/2024 Added by: [Helen Walton](#) Version: 1.3

 [organisationalStructure May22.pptx](#) Added: 23/11/2022 Added by: [Lindsay McLeod](#) (Deactivated) Version: 1.0

Linked work

No Links to display.

A.6.1.2: Segregation of duties

Assigned to: Jakub Szerszen

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Open

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:
No Categories to display

Added by Helen Walton on 08/05/2024 at 15:56

What we do

The segregation of duties is used to ensure conflicting responsibilities are not allocated to the same individual and to prevent a single individual being able to access, modify or use assets without authorisation or detection.

We implement segregation of duties through defined roles and responsibilities as defined in [\(A.6.1.1\) Information Security Roles & Responsibilities](#).

Additional segregation is implemented through our [Access Control Policy \(A.9.1.1\)](#) and supports our [Information Classification Policy \(A.8.2.1\)](#) using the principles of:

- “Deny-by-default”
- “Need-to-know”
- “Least privilege”
- Role-based Access Control (RBAC)

Given the small size of the organisation, personnel may have multiple roles. Where appropriate the individual will switch user/administration log-ons to prevent risk of error.

Note that the specific ISMS role requirements below are complementary and additional to those described in [5.3 Roles and Responsibilities](#).

Current Segregation of Duties

DevOps	The devOps team is having the responsibility of securing data and information from any kind of violations in the form of theft, abuse or loss - whether it is while storing it, transferring it or using it. These objects are expected to be achieved by: • Assessing the system’s security controls and processes to find potential security gaps • Planning changes and upgrades for corporate IT infrastructure • Maintaining system integrity • Implementing insider threat control measures • Choosing new security software if needed • Implementing disaster recovery measures • Analyzing previous incidents and creating an incident response plan • Analyzing the costs and benefits of security solutions
Artists	Artists are expected to consider ISMS in terms of their personal access to the company's systems as well as in any role connected to change management. They have responsibility for the security of digital assets and IP (both our own and those we may licence from others).

	Designers are the most likely role to keep data and assets locally on their machines or hard-drives (due to size constraints). As such they must be very aware of the security of their working space, the need for back ups and up-to-date virus software.
Developers	As a part of software development, code should be developed in line with good practice, so it can be extended and maintained effectively and therefore developers are being encouraged to: • Implementing User Acceptance Criteria to have stakeholders affirm the project is up to standard; • Code reviews; • Clear coding standards and guides; • Testing of all code; • Appoint a dedicated Product Manager to monitor the quality of the project and take ownership to all stakeholders for the success and failures; and • Maintain up-to-date documentation • Setting responsibilities for stakeholders • On-board new or replacement stakeholders with a learning guide • Open clear lines of communication between stakeholders by valuing transparency and honesty • Record or document meetings and action items that may arise
Sales & Marketing & Operations	Sales and marketing team is in a particularly vulnerable position as most of the sales reps are in contact with dozens of customers and potential customers. Operations are also in contact with customers as part of onboarding, set up, rollout and first line support. These factors make them more likely to reveal sensitive data. The following precautions should be taken • Use only encrypted devices • Use best password practices • Use only secured wi-fi • Documents containing confidential or sensitive information should never be shared outside the company or with authorized parties. • All sales reps are responsible for setting file or folder permissions to ensure data is only accessible to the relevant authorized parties.
Producers	Producers / Project Managers are expected to consider ISMS in terms of their personal access to the company's systems as well as in any role connected to change management. As G Gaming is mainly a remote working company, producers should ensure all communication files and transferred data are stored safely. They must be very aware of the security of their working space, the need for back ups and up-to-date virus software.

Linked work

No Links to display.

A.6.1.3: Contact with authorities

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 15:09

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 14:14

What we do

Each authority has a nominated contact owner from within the organisation who is responsible for managing the relationship with the authority. This responsibility includes initiating and maintaining the relationship and ensuring that any contact information held in the relevant places is current and complete.

Contact with external parties, including authorities, is in accordance with their [Interested Party](#) position on the map and is done by the relationship owner.

Policy

The purpose of this policy is to ensure correct and efficient contact with relevant authorities by the nominated person(s) with approved responsibility.

Policy Statements

1. All staff have a responsibility to contact the emergency services in an emergency situation.
2. Only those nominated to contact authorities outside of emergency situations may do so.
3. If the nominated individual is not available escalation must be made to board level.

Defined contact with authorities

The following table details the defined responsibilities for contacting specific authorities:

Authority	Responsibility
Emergency Services	Anyone - in an emergency situation.
Non-emergency Police (e.g. for reporting crime)	Chief Technology Officer

19/12/2024, 11:31ISMS.online ISO 27001 Policies & Controls

Information Commissioner's Office (ICO)	Data Protection Officer (DPO)
Financial regulators (e.g. FCA)	Chief Financial Officer
Other (non gambling licence) public sector regulators such as the ASA	Members of the Management Review Board
Licensing bodies: UKGC, MGA, DGA etc	Chief Financial Officer; third party legal representatives or third party accredited test houses as instructed

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.6.1.4: Contact with special interest groups

Assigned to: Helen Walton
Days estimated: 0.0
Days taken: not set
Due: not set
Status: Completed
Approved by Helen Walton on 07/05/2024 15:12
Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.
Categories:
No Categories to display
Added by Helen Walton on 07/05/2024 at 15:11

What we do

We encourage memberships of professional bodies, and security and industry specialist forums, by any member of staff.

Where appropriate information-sharing and confidentiality agreements are established.

We also consider hardware and software vendors as special interest groups in regard to security vulnerability patch and configuration management.

Policy

Contact with special interest groups must obey our [Code of Conduct](#) and [Acceptable Use Policy \(A.8.1.3\)](#).

Special Interest Groups

Special Interest Group	Purpose of contact
National Cyber Security Centre	Latest advice & guidance related to Cyber Security: https://www.ncsc.gov.uk NCSC Weekly Threat Reports NCSC Recent Incident Reports & Advice
Cyber Security Information Sharing Partnership (CiSP)	Cyber Security Information Sharing Partnership (CiSP)
Information Commissioner's Office	Privacy & data protection guidance for organisations
SANS Institute (SysAdmin, Audit, Network and Security)	SANS Weekly Bulletins & Alerts SANS Information Security Reading Room
AWS (Amazon Web Services)	Documentation relating to AWS including security of its Cloud Services
Google Cloud	Documentation relating to Google Cloud security
EGR Compliance	https://egr.global/compliance/ Specialist news regarding industry compliance topics
National Gaming Regulators	clarification around new regulations, licensing updates; industry forum; consultations

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.6.1.5: Information security in project management

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 15:14

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 07/05/2024 at 15:13

What we do

When starting any project (whether a new type of product development, an integration or other service), users must:

- Consider information security objectives as part of the project objectives. (Part of the kick-off meeting - as examples, both Crash and Flake are deemed higher risk projects due to their multiplayer nature and use of more novel technology)
- Ensure that information security requirements are set before selecting or developing a solution in line with controls in [\(A.14\)](#) System Acquisition, Development and Maintenance.
- Where relevant, use an integrated ISO 27001 CIA based risk assessment and treatment plan to evaluate and address specific project risks over the life of the project and align with existing ISMS controls.
- Report back to the Management Review Board or through other relevant channels if the project identifies bigger picture information security risks or issues that would be considered as relevant for the ISMS but are not yet included in the ISMS overarching risk register.
- Review information security objectives and requirements throughout the project lifecycle and adjust risk treatment to ensure controls are adequate and proportionate. (Part of the rollout/signoff checklist)

Linked work

No Links to display.

A.6.2 Mobile devices and teleworking. Objective: To ensure the security of teleworking and use of mobile devices.

A.6.2.1: Mobile device policy

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Dan Rough on 08/03/2022 12:36

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 28/02/2022 at 19:49

What we do

The Mobile Device Policy has been implemented to allow personnel to work away from organisational office locations in a secure manner and does not seek to impose restrictions that are contrary to the organisation's established culture of openness, trust and integrity.

Staff joining G Gaming are offered the opportunity to use a machine of their own choosing. The intention behind this is to ensure that all staff members have a machine that is appropriate for the job they do.

This policy addresses the security and confidentiality of G Gaming's data that will be accessed using devices that are the property of staff members.

The data that G Gaming collects plays a role in supporting business processes and customer services, in contributing to operational and strategic business decisions and in conforming to legal and statutory requirements.

Accordingly, the information and the enabling technologies are important assets that will be protected to the level commensurate with their value to the organisation. Special care will be taken to ensure that Person Identifiable and business/corporate confidential information is not compromised.

Nothing in this policy affects G Gaming's ownership of corporate information, including all work-related intellectual property created in the course of business using a personally owned device.

The organisation sets the controls applicable to business information stored or processed by mobile devices based on the information classification set out in [\(A.8.2.1\) Classification of Information](#)

Policy

The purpose of this policy document is to ensure that all staff are aware of their individual responsibilities in relation to the security and confidentiality of data which G Gaming holds and how that may be accessed using devices that they own.

This policy applies to the following mobile devices:

- Laptops
- Tablets
- Smartphones & Smartwatches

Policy Statements

Use of mobile devices

1. All devices that process our information whether provided by the organisation or personally owned must be recorded in the asset inventory.
2. Information must not be stored locally but on the company dropbox account or in one of our approved tools such as github or notion.
3. Authorised employees of G Gaming are responsible for the implementation of this policy in relation to the use of devices owned by them and used to access G Gaming's networks or systems.

Technical requirements

1. Devices must use the most recent stable version of the operating system (OS) available.
2. Remote wipe capabilities must be enabled if available.
3. Anti-virus and anti-malware software must be enabled wherever possible and must be approved by the TISO.
4. Devices must not be "jailbroken" (i.e. remove limitations imposed by the manufacturer or supplier) or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
5. Devices must automatically lock after no more than 5 minutes of inactivity, ideally less.
6. Devices must store all user-saved passwords in an encrypted password store.
7. If a password or passcode is used to unlock devices, it must meet organisational standards for length and complexity.
8. If a password manager is used, then:
 - a. the password manager must require the entry of another password or passcode before auto-filling forms with authentication credentials
 - b. in order to access the password vault fully the user must enter a password that meets organisational requirements for master passwords, see [\(A.9.3.1\)](#).
9. Other mechanisms for unlocking devices (e.g. fingerprints) must be approved by the TISO.

User requirements

1. Users must only load data essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to IT immediately.
3. If a user suspects that unauthorised access to company data has taken place via a mobile device the user must report the incident in alignment with the organisation's [Incident Management Policy \(A.16.1.1\)](#).
4. Users must not load pirated software or illegal content onto their devices.

5. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden.
6. Devices must be kept up to date with manufacturer or network provided patches. As a minimum, patches must be checked for weekly and applied at least once a month.

7. Staff wishing to use personally owned devices to connect to G Gaming's networks and systems MUST agree to the following:

G Gaming will not be held liable for any loss of personal data the user may incur, either through the installation of the application on their device or as a result of actions taken by G Gaming to ensure the security of its data, such as wiping, should the user's device be lost.

User acceptance

1. Where requested, MUST allow their mobile device to be audited to ensure compliance with policy. This may entail accessing personal data
2. MUST allow G Gaming to remotely wipe data from the device should it be lost
3. MUST accept full liability for any data breach should they fail to comply with the terms of this policy
4. Where appropriate, MUST accept to the device being provisioned by G Gaming so that a known set of software is installed
5. MUST ensure that the anti-virus and remote wipe software that is installed by G Gaming on an applicable device will not be removed, nor prevented from running at any point
6. MUST allow G Gaming to audit the device to review its logs

"Confidential" information

The following policy statements apply to information classified as "Confidential" in line with our [Data Classification Policy \(A.8.2.1\)](#)

1. "Confidential" information is permitted on mobile devices provided Master content is held on the designated system (e.g. CRM, Help Desk etc)
2. Synchronization with a cloud-based storage service (e.g. iCloud, google drive, etc.) is permitted but the access to the information stored by the service must meet the relevant controls in the ISMS (e.g. password strength).
3. "Sensitive" information may only be stored, processed or accessed on devices owned and controlled by the organisation.

"Sensitive" information

Trusted networks (Wi-Fi or hard-wired)

A "trusted network" is one that meets organisational requirements and is controlled by:

1. our organisation
2. one of its employees or associates
3. a trusted person of the employee or associate (e.g. a family member or friend)

Use of untrusted networks (Wi-Fi or hard-wired)

An “untrusted network” is any network other than those defined as “trusted” above.

1. Devices may only connect to untrusted networks providing an approved VPN (Virtual Private Network) technology is used for all communications.

Use of mobile hotspots

1. The use of mobile hotspots is allowed provided it is either your own or that of a trusted associate.

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#)

Linked work

No Links to display.

A.6.2.2: Teleworking

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Dan Rough on 08/03/2022 12:36

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 28/02/2022 at 19:50

What we do

The organisation has been designed with teleworking as a part core of the way work gets done. There are many controls in the ISMS which, when combined, robustly deal with the risks associated with teleworking. These controls include:

- [\(A.6.2.1\) Mobile device policy](#)
- [\(A.8.3.1\) Management of removable media](#)
- [\(A.8.3.3\) Physical media transfer](#)
- [\(A.9.3.1\) Use of secret authentication information](#)

- (A.9.4.2) Secure log-on procedures
- (A.10.1.1) Policy on the use of cryptographic controls
- (A.10.1.2) Key management
- (A.11.2.8) Unattended user equipment
- (A.11.2.9) Clear desk and clear screen policy
- (A.12.2.1) Controls against malware
- (A.13.1.1) Network controls

Linked work

No Links to display.

A.7. Human Resource Security

A.7.1 Prior to employment. Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

A.7.1.1: Screening

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 07/05/2024 16:28

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 07/05/2024 at 15:29

What we do

Our recruitment and onboarding process details the screening activities that are to be undertaken for all new hires where appropriate. Our adverts and hiring processes also alert candidates in advance about our certifications and requirement for screening (without being insensitive or creating barriers).

Our screening processes include:

- Availability of satisfactory character references, e.g. one business and one personal;
- A verification (for completeness and accuracy) of the applicant's curriculum vitae
- Confirmation of claimed academic and professional qualifications (where relevant)
- Independent identity verification (passport or similar document)
- Character and criminal disclosure record where required for any relevant staff

When an individual is hired for a specific information security role, we also make sure the candidate:

- Has the necessary competence to perform the security role;
- Can be trusted to take on the role, especially if the role is critical for the organisation

Senior managers in the organisation undertake verification reviews and specialist team members undertake interviews with candidates. Where team working is vital and close collaboration needed, we may also invite the candidate for a 'pairing' interview where they work together collaboratively with a colleague for a workshop session.

Contractors who have access to sensitive information or are performing roles where they might impact our information security, for example freelancers, are brought on using a similar process.

For some roles involving handling sensitive government information, additional vetting takes place where we may seek Security Clearance (SC) (or make achieving that once hired) conditional as part of the role.

Linked work

No Links to display.

A.7.1.2: Terms and conditions of employment

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:08

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 28/02/2022 at 21:00

What we do

Our standard terms and conditions of employment are attached. They are deliberately user friendly and easy to read.

They are supplemented by

- Our employee handbook held and regularly updated in Notion
- Our policies and procedures which related Data Classification and Management
- The organisation's [Code of Conduct](#)

We draw particular attention to

- Non-disclosure and confidentiality;
- Clarity over copyright and other assets;
- Data protection;
- Handling of information in particular information marked "Confidential"
- Actions and consequences for disregarding information security requirements and the possible use of the disciplinary process detailed in ([A 7.2.3](#)); and

Evidence of staff accepting the terms and conditions is given when they sign the contract.

Documents



[G Employment Contract G Gaming.pdf](#)

Added: 05/12/2022 Added by: [Lindsay McLeod](#)

(Deactivated) Version: 1.1

Linked work

No Links to display.

A.7.2 During employment. Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

A.7.2.1: Management responsibilities

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:13

Confidential

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 08:09

What we do

G's leadership responsibilities include ensuring that employees, relevant contractors and suppliers:

- a) are properly briefed on their information security roles and responsibilities prior to being granted access to organisation information or information systems;
- b) are provided with guidelines to state security expectations of their role within the organisation;
- c) are motivated to fulfil the security policies of the organisation;
- d) achieve a level of awareness on security relevant to their roles and responsibilities within the organisation
- e) conform to the terms and conditions of employment, which includes the organisation's information security policy and appropriate methods of working;
- f) continue to have the appropriate skills and qualifications

Our organisation achieves this in five ways:

1. [Employment terms and conditions \(A.7.1.2\)](#)
2. Our onboarding processes - including a buddy and check in processes
3. Ongoing personal development and delivery through collaboration within a related group of roles including away days, workshops and regular review meetings
4. All staff are also members of our shared messaging and information tools Slack and Notion.
5. For other contractors and suppliers their responsibilities are defined as part of the specific contract.

Points 2 and 3 reinforce compliance to the code of conduct and all other relevant controls from this ISMS. Where training is required this is also addressed with supporting materials as required including those outlined in [\(A.7.2.2\)](#).

Whistleblowing

Under part g) of the ISO 27002 guidance, staff should be provided with an anonymous reporting channel to report violations of information security - "whistleblowing".

The organisation believes that following its risk assessment and cultural considerations, as well as current size, the need for anonymous reporting outside of the existing formal support channels, and the informal channels of meetings and calls, is very low so does not warrant investment in a specific technology solution per se. However we do have a specific policy (attached). To comply with ISO 27001: 2013 staff are advised that if they wish to anonymously report security incidents the following applies:

- Ask a trusted friend who is not known to the organisation to ring a director of the organisation and share the concerns, without revealing the name of the employee.

- The director will then act on that information as per any other security incident.

Anonymous reporting by customers and other Interested Parties is not something we anticipate needing a specific channel for either. Given the contractual nature and type of information services being delivered with our solutions, any breaches or concerns of information security in the delivery of the service would come through our existing support channels and mean immediate escalation to the appropriate member of the Management Review Board.

Documents

 [Whistleblowing_Policy_G_Games.docx](#) Added: 08/05/2024 Added by: [Helen Walton](#) Version: 2.0

Linked work

No Links to display.

A.7.2.2: Information security awareness, education and training

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:20

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 08:16

What we do

Information security awareness, education and training is delivered to staff and, where necessary, contractors and other interested parties as part of their induction to the organisation.

The attached ISMS policy document is shared with all new employees and a copy is held on our shared documentation resource Notion. <https://www.notion.so/gluckgam...>

Ongoing training and awareness is ensured when a key policy which impacts staff is changed, an update is delivered by the Management Review Board onto Notion and to the Slack channel "Important" which alerts all staff.

In addition, the regular team meetings have an update on anything of relevance around information security and reinforce key principles.

Every employee is a member of that Group regardless of their role. The Group is administered and curated by the Data Protection Officer and the relevant information security specialists. The Group communications and awareness mechanisms include:

- **Notes** - All general communications and awareness work that simply needs to be broadcast to staff is done by posting a note to the company's communication channels on Slack. This can include basic information updates such as latest news on data protection, information security updates and hot topics, including links off the platform e.g. to become aware of latest guidance from the ICO emerging as GDPR knowledge and practice matures.
 - **Policy Changes** - Any changes to policy documents which are deemed to be significant may require staff to re-read and re-accept the policy packs using the ISMS online Policy Pack tool. The decision on this will be made by the Management Review Board following the annual review of Policies or three year audit cycle, or following feedback from a third party audit. The policy pack send out and signing process will then be triggered.
 - **Discussions** - are used to provide multi-way engagement with staff, for example requesting feedback on proposed changes to systems and consulting around privacy impact assessments, through to the DPO or info sec specialists receiving and answering questions for the benefit of one or more people then retaining it as evidence and knowledge management.
 - **Tasking** - is used in the Group to demonstrate compliance with a requirement or to delegate down a piece of work to others and visibly show that having been completed. Tasking can be set for an individual through to all members of the Group at once. The organisation uses tasks for the team when there are material changes they need to comply with e.g. fundamental change to a key policy, or an annual reminder for compliance of the whole system. All tasks are timestamped, and audit trailed.
 - **Documents** added into Notion provide a means for sharing files and related information to that audience. Examples include the ISMS onboarding page linked to above
-
- [ICO website](#)
 - [ICO YouTube channel](#)
 - [National Cyber Security Centre](#)

Where relevant the Group administrators will post updates using one of the communication mechanisms above depending on the interaction and compliance required.

The ISMS Group and introductory communications around data protection and information security are complemented by specialist induction, training and other support as required for individuals and teams, depending on their role and access to valuable information such as data subject personal details. Evidence of that specific awareness and training is held in the relevant HR records or department training environment.

The [Terms & condition of employment \(A.7.1.2\)](#) and [Code of Conduct](#) provide the foundation awareness for information security to which staff must adhere. Failure to do so may lead to investigation and action in accordance with the [Disciplinary process \(A.7.2.3\)](#).

Documents

 [GDPR_and_infosec_intro_training.pptx](#) Added: 28/02/2022 Added by: [Helen Walton](#) Version: 4.0

Linked work

No Links to display.

A.7.2.3: Disciplinary process

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:20

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 01/03/2022 at 10:43

Disciplinary Process

Purpose and Scope

This process is designed to ensure that all employees are aware of and understand their rights and responsibilities relating to discipline. It aims to facilitate satisfactory standards of conduct and performance, to encourage improvements where appropriate and to ensure that cases of alleged misconduct, unacceptable performance or other acts or omissions considered by management to warrant consideration of disciplinary action are dealt with consistently and fairly within a reasonable timescale.

The process applies to all employees of the organisation except Company Board Members.

Our rules and policies relating to the conduct of employees have been drawn up to set standards of behaviour and performance at work and to deter acts of misconduct. These can be found within various documented policies in this ISMS, including our [Code of Conduct](#) and Information Security Policies, and they aim to encourage employees to achieve and maintain high standards of discipline, behaviour and performance. Any breaches may be dealt with as a disciplinary matter under the provisions of this process.

Note: The process does not apply to termination of employment:

- arising from the conclusion of the employment for which an employee was specifically appointed where the term or need for such an appointment has expired or is about to expire;
- during or at the end of a period of probationary service;
- by reason of redundancy;
- arising from ill-health.

Principles

All senior or experienced staff are responsible for identifying promptly any deficiencies in conduct or performance, discussing the matter with the individual member of staff and assisting him/her to improve. Minor matters will normally be dealt with informally.

The organisation reserves the right to implement the process at any stage as set out below taking into account the alleged misconduct of an employee. Employees will not ordinarily be dismissed for a first disciplinary offence.

Where time limits are referred to in the course of this process, they may be varied by agreement between the employee and the organisation.

Employees have the right to be accompanied at a formal disciplinary hearing by a fellow worker or trade union official of their choice.

Matters that the organisation views as amounting to disciplinary offences include (but are not limited to):

- failure to observe or comply with the organisation's policies, standards, procedures and processes, in particular those around information security and privacy;
- abusive behaviour;
- behaviour likely to bring the company into disrepute;
- unreasonable refusal to follow an instruction issued by a manager, supervisor or director;
- poor attendance, and
- bribery offences under the Bribery Act 2010.

Informal Process

In many circumstances it will not be appropriate to proceed immediately to the formal disciplinary process.

Minor cases of misconduct may best be dealt with by informal advice, coaching and support rather than through the formal disciplinary process. Managers should discuss problems with individuals with the objective of encouraging and helping them to improve. It is important that employees understand what needs to be done, how conduct will be reviewed and over what period. Employees should also be made aware of what action may be taken if they fail to improve their conduct.

Performance

If an employee's performance does not meet acceptable standards after attempts to resolve matters informally, a performance improvement policy should be followed. Its purpose is to provide a framework for resolving the issue, ideally through the improvement of the employee's performance. As a last resort, the policy specifies the circumstances in which the employee may be redeployed to more suitable work or dismissed on the ground of capability.

Formal Process

Investigation

A supervisor or manager will be appointed for the employee. This manager will then promptly and thoroughly investigate any matter that is reasonably suspected or believed to contravene any of the organisation's policies or rules or may otherwise be a disciplinary matter. The employee will be informed as soon as possible as to the fact of an investigation and when it has been concluded.

There may be instances where suspension with pay is necessary while investigations are carried out. The organisation has the right to suspend with pay where there are reasonable grounds for concern that evidence may be tampered with, destroyed or witnesses pressurised before the disciplinary hearing, or if there is a potential risk to the business or other employees or third parties in allowing the employee to remain at work.

Employees who are suspended with pay need to be available during their contracted hours to respond to queries about any disciplinary matter and, but not limited to assisting managers with work related matters, attending disciplinary investigations/meetings.

Depending on the circumstances of the case, the employee may be invited to attend an investigatory interview. If such an interview is held prior to a disciplinary hearing, the employee will be informed at the outset that the interview is an investigatory interview.

There is no right for employees to be accompanied at a formal investigatory interview.

The organisation reserves the right to dispense with an investigatory interview and to proceed directly to a formal disciplinary hearing.

Procedure

Where, upon completion of an investigation, there are reasonable grounds to believe that an employee has committed an act of misconduct; the employee will be invited to attend a disciplinary hearing before the appointed manager or Director.

In the event of a disciplinary hearing taking place the organisation will:

- a) give the employee a minimum of two working days' advance notice of the hearing;
- b) tell the employee the purpose of the hearing and that it will be held under the Employer's disciplinary process;
- c) explain the employee's right to be accompanied at the hearing by a fellow worker or trade union official;
- d) give the employee written details of the nature of his/her alleged misconduct; and
- e) provide to the employee all relevant information (which should include statements taken from any fellow employees or other persons that the organisation intends to rely upon against the employee) not less than two working days in advance of the hearing.

Non-attendance of disciplinary meetings

Where the employee is unable to attend a disciplinary hearing and provides a good reason for failing to attend, the hearing will be adjourned to another day. The organisation will comply with (a) above in respect of giving notice of the rearranged hearing. Unless there are special circumstances mitigating against it, if the employee is unable to attend the rearranged hearing, the rearranged hearing will take place in the employee's absence. The employee's fellow worker or trade union official may attend in such circumstances and will be allowed the opportunity to present the employee's case. The employee will also be allowed to make written submissions in such a situation.

Where the chosen companion is unavailable on the day scheduled for the meeting, it will be rescheduled, provided that the employee proposes an alternative time within five working days of the scheduled date.

When an employee repeatedly fails to attend a disciplinary meeting, the organisation will look at the employee's reason for non-attendance; the employee's disciplinary and work record, seniority and length of service; the severity of the disciplinary issue; and any medical opinion on the employee's ability to attend the meeting. Where there is no good cause for the employee's repeated non-attendance, the panel can hold the meeting in the employee's absence, taking into account any written representations from the employee, and any other available evidence, before it makes a decision. The employer should give the employee the right to appeal the decision.

Role of companion

The employee's chosen companion has the right to address the hearing to put the employee's case, sum up the case and respond on the employee's behalf to any view expressed at the hearing. The companion may also confer with the employee during the hearing. However, there is no requirement for the employer to permit the companion to answer questions on behalf of the employee, or to address the hearing where the employee indicates that he/she does not wish this.

The disciplinary hearing

A disciplinary hearing will normally be conducted by the employee's appointed manager together with a senior manager or Director (the panel). Any member of management responsible for the investigation of the disciplinary offence(s) shall not be a member of the panel, although such managers may present any supporting facts and material to the disciplinary hearing. The employee will be entitled to be given a full explanation of the case against him/her and be informed of the content of any statements provided by witnesses. The employee will be able to call his/her own witnesses. He/she will be permitted to set out his/her case and answer any allegations. The employee will be given a reasonable opportunity to ask questions, present evidence and call relevant witnesses. He/she will also be given the opportunity to raise points about any information provided by witnesses. Where the organisation intends to call relevant witnesses it will give the employee advance notice of this. The employee must also give advance notice if he/she intends to call relevant witnesses.

The organisation may adjourn the disciplinary proceedings if it appears necessary or desirable to do so (including for the purpose of gathering further information). The employee will be informed of the period of any adjournment. If further information is gathered, the employee will be allowed a reasonable period of time, together with his/her fellow worker or trade union official, to consider the new information prior to the reconvening of the disciplinary proceedings.

As soon as possible after the conclusion of the disciplinary proceedings, the employee's line manager will convey the decision of the panel to the employee and will also inform the employee what disciplinary action, if any, is to be taken. The decision will be confirmed in writing. The employee will be notified of his/her right of appeal under this process.

Disciplinary action

Where, following a disciplinary hearing, the organisation establishes that the employee has committed a disciplinary offence, the following disciplinary action may be taken:

a) Where a minor offence or offences have been committed, a personal development plan (PDP) recorded oral warning may be given. The warning will ordinarily state that any further misconduct will render the employee liable to further, more severe disciplinary action. The employee should be informed of the period that the warning will remain "live". During this period, the organisation may rely on such a warning in the event of further misconduct on the part of the employee.

b) Where either a more serious disciplinary offence has been committed or further minor offences have been committed by an employee following a recorded oral warning that remains "live", the employee will receive a first written warning within their PDP. The warning will:

- a. set out the nature of the offence committed;
- b. inform the employee that further misconduct is liable to result in further disciplinary action under this process;
- c. specify the period for which the warning will remain "live", after such period the organisation will review the warning; and
- d. state that the employee may appeal against the warning.

- e. a final written warning will be removed from the PDP file and disregarded for disciplinary purposes after a period of 24 months, subject to satisfactory conduct and performance within that period.
- c) Where a serious disciplinary offence amounting to gross misconduct has been committed, thereby justifying summary dismissal, but the organisation decides, after taking into account all appropriate circumstances, that a lesser penalty is appropriate, or, where an employee commits further disciplinary offences after a first written warning has been issued and remains "live", a final (or combined first and final) written warning may be given within their PDP. Such a warning will:
 - a. set out the nature of the offence committed;
 - b. inform the employee that further misconduct is likely to result in his/her dismissal; and
 - c. state that the employee may appeal against the warning.
- d) Where the employee has committed further acts of misconduct (these being acts of misconduct other than gross misconduct) following a final written warning given under c. above, the employee may be dismissed with notice or with pay in lieu of notice.
- e) Where the organisation establishes that an employee has committed an act of gross misconduct, the employee may be summarily dismissed.
- f) Where a final written warning is given within their PDP to an employee under c. above, the organisation may also impose on the employee:
 - a. disciplinary suspension;
 - b. demotion;
 - c. in line with any provision in the contract of employment, transfer to a job of a lower status.

The above sanctions may be imposed in conjunction with other forms of disciplinary action, or as an alternative to dismissal.

Appeal

An employee may appeal against any disciplinary sanction imposed against him/her, with the exception of an informal oral warning.

The appeal will be heard by the CEO and/or the Finance Director, whoever has not been involved in the decision to impose the disciplinary sanction on the employee.

The senior manager(s) hearing the appeal is/are obliged to consider any representations made by the employee, the employee's fellow employee or trade union official and those of the manager who conducted the investigation and the manager who conducted the disciplinary hearing and imposed the disciplinary sanction.

The senior manager(s) hearing the appeal must decide on the basis of both sets of representations, together with any subsequent facts that may have come to light, whether or not to uphold the disciplinary sanction.

In the event that the senior manager(s) finds for the employee, the senior manager(s) shall allow the appeal and shall remove all records of the disciplinary sanction from the employee's PDP record.

In the event that the senior manager(s) does not accept the representations made by or on behalf of the employee, the senior manager(s) must uphold the disciplinary sanction.

When lodging an appeal, the employee should state:

- a) the grounds of appeal; and
- b) whether he/she is appealing against the finding that he/she has committed the alleged act or acts of misconduct, or against the level of disciplinary sanction imposed.

The employee must provide written notice of the appeal within five working days of being informed of the disciplinary sanction being imposed against him/her.

Appeal hearings will normally take place within 14 days of receipt of the employee's written notice of appeal.

Upon completion of the appeal, the senior manager(s) conducting the hearing will convey his/her decision to the employee. The decision will be confirmed in writing within their PDP inside one week. The organisation's decision at the appeal is final.

Where an appeal lies against a dismissal by the panel, the panel's decision to dismiss will have had immediate effect and, therefore, if the dismissal is by notice, the period of notice will already have commenced on the date that the decision was given by the panel. If the panel's decision was to dismiss the employee summarily without notice, the organisation will be under no obligation to reinstate or pay the employee for any period between the date of the original dismissal and the appeal decision and the original date of termination will stand. In the event that the panel's decision to dismiss is overturned, the employee will be reinstated with immediate effect and he/she will be paid for any period between the date of the original dismissal and the successful appeal decision. His/her continuous service will not be affected.

Gross Misconduct

Gross misconduct is misconduct of such a serious and fundamental nature that it breaches the contractual relationship between the employee and the organisation. In the event that an employee commits an act of gross misconduct, the organisation will be entitled to terminate summarily the employee's contract of employment without notice or pay in lieu of notice.

Matters that the organisation views as amounting to gross misconduct include (but are not limited to):

- theft, misappropriation or unauthorised possession of the assets, funds, equipment and/or property of the organisation, employees or visitors,
- fraud, including any deliberate attempt to defraud the organisation, employees or other persons or organisations in the course of duties and responsibilities,
- corruption, including the acceptance of money, goods, favours or excessive hospitality from outside parties in respect of acts or service(s) rendered which are contrary to the interests of the organisation,
- deliberate falsification or misrepresentation of records or claims made,
- physical violence towards fellow employees or visitors,
- deliberate damage to property belonging to the organisation, employees or visitors,
- serious negligence or breach of safety rules potentially causing unacceptable loss, damage or injury,
- flagrant disregard of the organisation's policies, standards, processes, procedures, regulations or rules in force from time to time including Copyright (or other rights) infringement of any third Party .
- serious acts of insubordination, including flagrant refusal to comply with a reasonable instruction.
- serious misuse of the organisation's property, facilities or name,
- acts or omissions which might damage the organisation's operations and/or which bring the organisation into serious disrepute.
- serious breach of Information Security that may have financial or reputational consequences.

- other offences of dishonesty;
- conviction of a criminal offence that is relevant to the employee's employment;
- discrimination or bullying/harassment of a fellow worker on the grounds of sex, sexual orientation, race, disability, age or religion or belief.
- sexual misconduct at work;
- serious incapability at work or on duty through alcohol, possession, custody or control of illegal drugs on the organisation's premises;
- gross negligence;

Other acts of misconduct may come within the general definition of gross misconduct.

Miscellaneous

Ordinarily, if an employee who is an accredited representative of a trade union recognised by the organisation for collective bargaining purposes is suspected of having committed a disciplinary offence, the organisation will take no action under this process (with the exception of suspending the employee in a case of suspected or known gross misconduct) until the organisation has had a chance to discuss the matter, with the prior agreement of the employee, with a full-time official of that trade union. However, as an SME, the organisation does not currently recognise any trade union for collective bargaining purposes, although this may change in the future.

Linked work

No Links to display.

A.7.3 Termination and change of employment. Objective: To protect the organisation's interests as part of the process of changing or terminating employment.

A.7.3.1: Termination or change of employment responsibilities

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 18/01/2023 16:23

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Lindsay McLeod on 18/01/2023 at 16:10

What we do

In the event of termination of employment, issues such as non-disclosure and behaviour around confidential information after leaving the organisation are addressed in accordance with the [Terms and conditions of employment \(A.7.1.2\)](#).

The organisation also undertakes a professional exit project using a consistent repeatable set of activities for all leavers including employees and contractors that have been previously been given access to information and assets that has been marked "Confidential" or above.

A leavers checklist template has been created on our HR Trello Board, a sample of this checklist is attached below. A new card is created using this template each time an employee resigns.

A leaver's interview is held using a set of questions, a copy of these are attached.

Changes of employment that impact access to information or assets will be addressed within any induction to include addition or removal of the staff member from systems and processes as required and any relevant training given on the job by colleagues thereafter.

Documents

 [Leaver checklist, Trello](#) Added: 18/01/2023 Added by: [Lindsay McLeod](#) (Deactivated) Version: 1.0

 [Exit Interview Questions.docx](#) Added: 05/12/2022 Added by: [Lindsay McLeod](#) (Deactivated) Version: 2.0

Linked work

No Links to display.

A.8. Asset Management

A.8.1 Responsibility for assets. Objective: To identify organisational assets and define appropriate protection responsibilities.

A.8.1.1: Inventory of assets

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:21

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 15:12

What we do

We operate an [Information Asset inventory Tracker](#) that is updated dynamically as information assets change over the course of their life.

The tracker enables a single location for content updates, tasks, alerts and reminders, as well as links to risks, policies and controls. These are used as needed to ensure that the information asset is protected and reviewed regularly (at least annually or when change is required).

The inventory includes the following which are then used in developing the automated reports, statistics and insights from the tracker that can help decision making and management reviews:

- **Type** of information asset (e.g. financial information, IPR, infrastructure, personal data, information processing devices, products & services, removable storage/hard drive, sales and marketing information, software applications, supply chain, commercial /contractual information, other information);
- **Description** of the information asset to fit within the category above (e.g. Customer personal data) along with any further description to clarify scope;
- **Information Classification** (in accordance with [\(A.8.2.1\)](#)) to help demonstrate the value of the information and its protection level required for the policies and controls applied to protect or harness the asset in practice;
- **Financial value of the asset** – This is not mandated, however, The Management Review Board may optionally choose to add this to help illustrate financial value at risk and total value for the portfolio of assets;
- **Primary location** of the asset.
- **Legal owner** of the asset (which can include the organisation, employees (e.g. for BYOD devices), supplier/s, customer/s (in line with [\(A.8.1.2\)](#)))
- **Internal lead owner** of the asset who is responsible for ensuring it is protected adequately.

Information assets are tagged as “live” or, when decommissioned and no longer in use, as “resolved”. Following decommissioning, they are held as archived assets for audit and reporting purposes.

--

Linked work

No Links to display.

A.8.1.2: Ownership of assets

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:22

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 15:35

What we do

Asset ownership is categorised at two levels within the organisation as described in [\(A.8.1.1\)](#) and demonstrated on the [Information Asset Inventory Tracker](#):

- Legal owner (e.g. organisation, employee, customer, supplier)
- Lead asset owner (accountable for the asset category e.g. Devices, Software)

Assignment of ownership

The Lead Asset Owner is defined at the point of creation of a new asset category and the lead asset owner is responsible for:

- Ensuring that assets are inventoried;
- Ensuring that assets are appropriately classified and protected in accordance with [\(A.8.2.1\)](#);
- Defining and periodically reviewing access restrictions and classifications to important assets, taking into account applicable access control policies; and
- Ensuring proper handling when the asset is reused or disposed of.

These responsibilities may be delegated to other members of staff as appropriate (for example; updating the asset register or deleting assets during employee exit).

Asset responsibility is defined at the point where a member of staff is issued with that asset and the inventory updated accordingly.

Linked work

No Links to display.

A.8.1.3: Acceptable use of assets

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:23

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2022 at 12:52

What we do

We are a progressive organisation and expect all staff and representatives to operate to professional working practices and in particular comply with the [Code of Conduct](#) as well as the relevant information security policies in this ISMS.

To that end we do not lock down or limit website or broadband access, restrict email or prevent reasonable use of other services. Nor do we set out policies that prevent flexible working or the ability of our staff to use their work assets for personal use, as long as they are within the policies in the ISMS and the [Code of Conduct](#).

Staff are permitted to use their own information processing devices for work (BYOD) and we do not wish to prejudice some workers over others, but all staff must understand that anything defined as unacceptable or non-compliant with the policies in the ISMS or the Code of Conduct may be dealt with in accordance with the [Disciplinary Process \(A.7.2.3\)](#).

Staff who may be concerned about the suitability of a personally owned device for processing work information *and/or* questionable personal processing of information can speak to the CTO.

As described in other policies and controls areas, the organisation has the ability and reserves the right to detect, monitor, and forensically audit unacceptable use of information, information networks and systems or other related assets and services.

Policy

The purpose of this policy is to set out the limited set of rules to which personnel must adhere in regard to use of the organisation's information, information networks & systems, and other related assets. It is also designed to protect employees from accidentally breaching legislation.

The Acceptable Use Policy does not seek to impose restrictions that are contrary to the organisation's established culture of openness, trust and integrity.

Senior management is committed to protecting the organisation's employees, customers and the organisation itself from illegal or damaging actions by individuals, whether deliberate or accidental.

Policy Statements

General Use & Ownership

1. All networks and systems, including but not limited to computer equipment, software licences, operating system licences, storage media, and network accounts are the property of the organisation or viewed as

- under the control of the organisation even where the actual ownership belongs to the third party controlling them.
2. Organisational systems are to be used primarily for business purposes in serving the interests of the company and of our customers in the course of normal operations.
 3. Personal use of organisational equipment and access to the Internet is permitted providing such use does not amount to “unacceptable use” defined below.
 4. Because of the need to protect the organisation's network, management cannot guarantee the confidentiality of personal information stored on any network device belonging to the organisation.
 5. Wherever possible, any information that users consider sensitive must be encrypted in line with the [Cryptographic Controls Policy \(A.10.1.1\)](#)
 6. For security and network maintenance purposes, authorised individuals within the organisation may monitor equipment, systems, and network traffic at any time.
 7. The organisation reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
 8. Employees must take all necessary steps to prevent unauthorised access to information.
 9. Employees and other authorised users:
 - a. must keep passwords and other security authentication information secure and not share accounts.
 - b. are responsible for the security of their passwords and accounts.
 10. All PCs, laptops and workstations must be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less
 11. Users must secure their devices whenever the device will be left unattended when not in a private working space such as a home office. This includes sensible security measures such as ensuring laptops are out of sight if left in a locked vehicle or hotel room and employing sensible security even in the home, including not leaving doors or windows unlocked and using an alarm when out.
 12. Special care must be taken to protect laptops and other mobile devices when an employee is travelling, visiting a co-working space or in a customer or supplier office. These include not leaving laptops unattended but carrying them with you.
 13. Posts by employees from an organisational email address to newsgroups must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the organisation unless posting is in the course of business duties.
 14. All equipment used by the employee should use approved virus-scanning software with a current virus database.
 15. Employees must use extreme caution before opening e-mail attachments received from unknown senders as these may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are prohibited. Employees may be exempted from some of these restrictions during the course of their legitimate job responsibilities.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

Unacceptable System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Any activity that is illegal under relevant local, national or international legislation.
2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the organisation.
3. The exporting of software, technical information, or cryptographic technology, in violation of international or regional export control laws.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Using an organisational computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any organisational account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication - Security breaches include, but are not limited to, accessing data to which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of the job role. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification is made to and authorised by the CTO
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job role.
12. Circumventing user authentication or security of any host, device, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example by executing a denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means.
15. Providing information about, or lists of, the organisation's employees to parties outside of the organisation.

Unacceptable Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or messaging whether through language, frequency, or size of messages.
3. Unauthorised use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within the organisation's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the

organisation or connected via the organisation's network.

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.8.1.4: Return of assets

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:24

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 16:45

What we do

Responsibilities for the return of assets are laid out in the Employee Handbook held on Notion.

G Kit

In most circumstances, when joining the company you are given the opportunity to work with the equipment you want to work with.

You can purchase any machine up to a value of £1,699 (inc VAT) - this amount changes from time to time and is currently based on the 2020 Apple MacBook Pro 13" M1, 16 GB Ram, 512 GB. Monitors and accessory costs are covered on top.

If you are not using these monitors, you can instead purchase up to £2,148 (Inc VAT - this amount also changes from time to time and is currently based on the 2020 Apple MacBook Pro 16" i5, 16GB Ram, 512GB.

Though this model is used for guidance, you can buy any model. If you want to spend more money, then you are expected to cover the additional cost unless an exception applies.

The company may occasionally choose to buy more expensive equipment, in this instance, the equipment is owned by the company, not the individual.

If you are 100% using your own equipment (laptop/monitors etc) and a permanent member of staff, then you are entitled to a £500/€500 payment to help cover expenses related to that machine.

You can replace this machine after three years (if your start date was September 2020 or later), as long as the new machine offers a significant performance improvement to your work and the original machine will then belong to you. We may suspend this at any time to manage money since the equipment is a major cost to the company or choose to pace out replacements when a new model comes out or if lots of people request replacements at once.

If you leave within three years, you can purchase your machine for the pro-rata time that you have been in the company.

At any time, we may make decisions outside of this policy to support people in the way they work, so the above should be considered a guideline rather than a strict rule.

Leaver's Checklist

When an employee leaves, the Leaver's Checklist is completed which includes a section to process and record asset return activity. The assets will then be updated accordingly in the [Information Asset Inventory Tracker](#).

Third Parties

If third parties are granted access to assets the contract will include an agreement on the return or destruction of those assets once the requirement for them has ceased. This is tracked within the relevant [supplier relationship account](#) or the [Information Asset Inventory Tracker](#) where the third party will be noted as the responsible party.

Linked work

No Links to display.

A.8.2 Classification of information. Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.

A.8.2.1: Data Classification

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:25

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 28/03/2023 at 13:59

What we do

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to G Gaming should that data be disclosed, altered or destroyed without authorisation. All of the data that G Gaming processes, stores or interacts with is sensitive to one degree or another.

The purpose of this policy is to establish a framework for classifying and handling data within G Gaming. The classification scheme that it sets out is based on the information's level of sensitivity, value and criticality to G Gaming.

This policy forms part of G Gaming's Information Security policy. The Information Asset Register lists the data which G Gaming has cause to come into contact with, and the classification of it.

If a need to process a piece of data arises, and that data does not fall into one of the categories described in the following table, it should be assumed that the data is Internal/Private and treated accordingly.

We have conducted extensive risk assessment and consideration of assets as regards confidentiality, integrity and availability. We also take note of ISO 27002 guidelines on labelling "The procedures can define cases where labelling is omitted, e.g. labelling of nonconfidential information to reduce workloads."

To that end, organisation-controlled documents, digital content and physical drives (e.g. standalone back-up drives) holding files need to be classified or marked with one of the following:

"Public"

Risk - None

Data should be classified as Public when it can be published anywhere, without any fear of risk to G Gaming and its affiliates. No controls are necessary to protect this data as unauthorised alteration or modification of Public data would not cause G Gaming and its affiliates problems.

Public data is not sensitive. Access to the data can be granted to anyone and can be published without restriction. The integrity of the data should however be checked regularly. All efforts should also be made to ensure that the data remains accurate over time. There is no impact on G Gaming should Public data not be available.

Examples of Public data include social media posts, comments on articles published on the internet.

"Open"

Risk - Low

Data should be classified as Open when the unauthorised disclosure, alteration or destruction of that data would result in little or no risk to G Gaming and its affiliates. While few controls are required to protect the confidentiality of Open data, some level of control is required to prevent unauthorised modification or destruction.

Open data is not considered sensitive; therefore, it may be granted to any requester or published without restrictions. The integrity of Open data should be protected. All efforts should be made to ensure that Open data remains accurate over time. The impact on G Gaming should Open data not be available is typically low, (inconvenient but not debilitating).

Examples of Open data include company profile information, marketing relating to any of the products that G Gaming offers

"Internal/Private"

Risk - moderate

Data should be classified as Internal/Private when the unauthorised disclosure, alteration or destruction of that data could result in a moderate level of risk to G Gaming or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public or Open data should be treated as Internal/Private data. A reasonable level of security controls should be applied to internal data.

Access to Internal/Private data must be requested and authorised. Access to Internal/Private data may be authorised to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department.

Internal/Private Data is moderately sensitive in nature. Often, Internal/Private data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on G Gaming should this information not be available when needed is typically moderate.

Examples of Internal/Private data include official G Gaming records such as financial reports, human resources information, and budget information.

"Confidential"

Risk - high

Data should be classified as Confidential when the unauthorised disclosure, alteration or destruction of that data could cause a significant level of risk to G Gaming and its affiliates. Examples of Confidential data include data protected by the Data Protection Act. The highest level of security controls should be applied.

Access to Confidential data must be controlled from creation to destruction, and will be granted only to those persons affiliated with G Gaming who require such access in order to perform their job ("need-to-know"). Access to Confidential data must be individually requested and then authorised.

Confidential data is highly sensitive and may have personal privacy considerations. In addition, the negative impact on G Gaming should this data be incorrect, improperly disclosed, or not available when needed is typically very high.

Examples of Confidential/Restricted data include customer/player transactional information, personal identification information and credit card numbers.

For personal employee information the label "Sensitive" has been added to Dropbox folders. This is not of higher risk than Confidential data, but it has been added to help employees understand the personal nature of the information included.

Linked work

No Links to display.

A.8.2.2: Labelling of information

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:27

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 08:27

What we do

See [Classification of information \(A.8.2.1\)](#) for the broad context of the information labelling and handling as regards how the organisation uses policies for reinforcing information classification where it is not feasible to do so e.g. in online services.

Public – Not labelled. Only “Public” if clearly for un-restricted release

Open - unauthorised disclosure offers very low risk

Internal/Private unlabelled information is treated as this level unless clearly for public release.

Confidential – disclosure would offer significant risk.

Note:

Due to the confidential nature of Project Flake, a codename is used internally and all information access to certain folders is tracked. This project sits outside of our normal labelling and dropbox system.

Linked work

No Links to display.

A.8.2.3: Handling of assets

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:29

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 12/12/2022 at 16:37

What we do

See [Classification of information \(A.8.2.1\)](#) for the broad context of the information labelling and handling as regards how the organisation uses policies for reinforcing information classification where it is not feasible to do so e.g. across business critical digital services.

Wherever possible the organisation avoids the creation of paper-based information assets itself and attempts to produce only digital information. Customers and others who receive that can print and share as they see fit based on their policies and procedures in accordance with the classification and any controls we have applied to the information.

Policy

Our aim is to ensure that:

1. Information is collected, processed, held, transferred and disposed of appropriately.
2. Staff are aware of their rights and responsibilities in relation to information handling.
3. Appropriate mechanisms are in place to ensure that those about whom G Gaming holds data are advised of their rights in relation to the gathering and processing of their personal data.
4. In formulating and reviewing G Gaming's processes and procedures on records management, due regard is given to the current legislative provisions for data protection, including the EU General Data Protection Regulations (GDPR) and such guidance as may be issued by the UK Information Commissioner.

Policy Statements

1. All information is to be handled in accordance with our:
 - a. [Terms & conditions of employment \(A.7.1.2\)](#);
 - b. [Acceptable use of assets policy \(A.8.1.3\)](#); and
 - c. [Code of Conduct](#).

Principles of Retention of Data

1. Data protection legislation sets out a number of data protection principles of good information handling. These state that personal data will be:
 - Processed lawfully, fairly and in a transparent manner in relation to individuals;
 - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
 - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
 - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

using appropriate technical or organisational measures.

2. Specific Retention Requirements

G Gaming will ensure that all data processing for which it is responsible will be conducted in line with these principles. Differing jurisdictions in which G Gaming operates have different requirements for how long some key data is held. G Gaming documents these differing jurisdictional requirements for compliance purposes and will follow the relevant requirements for each jurisdiction.

Basis for Processing

To be able to process personal data, a Data Controller must ensure that such processing falls within the lawful bases for processing set out in Article 6 of the EU General Data Protection Regulations (GDPR). These are:

- Consent – An individual has provided clear consent for the processing of their personal data for one or more specified purposes;
- Contract – The processing of the personal data is necessary to fulfil a contract that G Gaming has with an individual;
- Legal Obligation – Processing of data is necessary to comply with the law, other than to fulfil a contractual reason;
- Vital Interests – Processing of data is necessary to protect someone's life;
- Public Task – Processing is necessary for G Gaming to perform a public interest task or to fulfil its official functions, where the task or function has a clear legal basis; and
- Legitimate Interests – Processing is necessary for G Gaming's legitimate interests or the legitimate interests of a third party, unless the need to protect an individual's personal data overrides those legitimate interests.

At each point that G Gaming collects data, the lawful basis for processing will be made clear.

Fair Processing Notices

Any form used to collect information from an individual will contain a Fair Processing Notice, which will set out the purpose for which the information is being sought and the data protection arrangements that apply to the information provided. The text of all Fair Processing Notices (sometimes referred to as Data Protection Declarations or Privacy Notices) and will refer to the lawful basis for processing the data being collected.

The information contained within the Fair Processing Notice must be provided to the individual Data Subjects whose Personal Data we Process and we must ensure that the Privacy Notices are properly communicated to individuals at the point at which their Personal Data is collected. Where we receive Personal Data from a third party with whom we have a contractual relationship, we will check that the Personal Data was collected by the third party in accordance with Data Protection Law and on a basis which contemplates our proposed Processing of that Personal Data.

Data Minimisation

Under the data protection principles, we must ensure that Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. You may only Process Personal Data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties. Do not collect excessive Personal Data. Ensure that any Personal Data you collect

is actually required for the intended purpose for which you will Process it. You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised.

In designing and operating systems and processes, G Gaming will ensure that all data is held and processed at the minimum level required to fulfil its functions and to meet the purpose for which data is being processed. Systems and processes will be designed and implemented in a manner that allows access to data to be restricted only to those with an explicit and legitimate reason for access.

Accuracy

The data protection principles require that Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. You must ensure that the Personal Data you use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it.

Security, Integrity and Confidentiality

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

You must

1. perform your work duties in such a way as to protect the Personal Data that we hold;
2. follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You must also comply with the requirements of all Relevant Policies and Guidelines and any directions issued by the DPO; and
3. not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect the Personal Data

Individual Rights

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

- the right to rectification;
- the right to erasure (sometimes referred to as 'the right to be forgotten');
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision making including profiling.

All data processing will be undertaken by G Gaming in line with the rights of data subjects. However, data subjects should be aware that the rights listed above may be qualified, limited or modified by the legal basis on which particular data is processed. Further information on individual rights is available from the Information Commissioner's website at www.ico.org.uk.

Amendment

Where G Gaming proposes to introduce or amend new systems or working practices that have implications for its data protection arrangements, we will manage risk and consider what control measures are appropriate to ensure that data remains protected, and all processing remains compliant with the principles set out above.

Subject Access Requests

Data subjects or anyone who considers that s/he may be a data subject for G Gaming have the right to request details of any personal data about them held by G Gaming, whether this is held in electronic format or any manual records which form part of a relevant filing system. Such a request is called a Subject Access Request. G Gaming will acknowledge all requests upon receipt and will provide a full response within one month from the date of receipt, as required under data protection legislation. G Gaming is entitled to ask for such evidence as it may reasonably require to verify the identity of the individual making the subject access request, before any information is provided. G Gaming may refuse a request that is manifestly unfounded or excessive. Where this is the case, G Gaming will confirm why the request is being refused and will confirm the arrangements open to the requester to appeal the decision.

Data Sharing

In the performance of its duties in relation to the employment of staff and the services provided to Operators, G Gaming may be required to share information with external organisations. Example bodies with whom G may be required to share or give access to data include:

- HMRC
- Pension Funds
- Insurance Companies
- Regulators in the various jurisdictions G Gaming serves

In all such cases where data is shared externally, G Gaming will ensure that appropriate safeguards are in place in relation to any data shared through agreed protocols or data sharing agreements.

Disclosure of Data to Third Parties

G Gaming must ensure that personal data is not disclosed to unauthorised third parties which includes family members. All staff should exercise caution when asked to disclose any personal data held on another individual to a third party. Disclosure must be relevant to, and necessary for, the conduct of G Gaming's business and subject to all other controls laid out in this Policy.

Data Security

All personal data processed by G is only accessible to those staff who need to use the information in the performance of their role. Personal data is password protected and is subject to our IT Security Policy.

Breaches

The purpose of this policy is to ensure G Gaming's data protection arrangements are well understood, but it is important to recognise behaviours and actions that would be considered as breaches of the policy and the consequences of any such breach. The following occurrences are considered breaches of this policy:

- unlawful procurement of information by anyone not entitled to access such information;
- unfair processing i.e. processing information for a purpose other than that for which it was provided;
- processing of inaccurate information, particularly if information was known to be inaccurate or steps could have been taken to ensure accuracy;
- unlawful disclosure i.e. sharing of information with anyone not entitled to receive it or loss of any data subject to this policy;
- collection, storage or processing of inadequate, irrelevant or excessive information; and
- unlawful disclosure.

Any abuses of this policy by a member of staff may result in a formal written warning.

Breaches

All breaches or suspected breaches of the policy or any loss of personal or sensitive category data must be reported to a member of the senior management team as soon as it is discovered. Where a breach or loss of data is reported, this will be notified to the Chief Technology Officer who will be responsible for developing a Breach Management Plan, which will contain the four elements below:

- Containment and Recovery
- Assessment of Ongoing Risk
- Notification of Breach to Information Commissioner
- Evaluation and Response

GDPR also makes notification of a breach of data protection mandatory where this is likely to result in a risk for the rights and freedoms of individuals, with such breaches notified to the relevant supervising authority within 72 hours of an organisation becoming aware of the breach

Consequences of Beach or Loss of Data

Staff should be aware that the penalties for a breach of the General Data Protection Regulation (GDPR) are significant and can include a fine of up to 2% of global turnover or €10 million (whichever is greater) or a fine of up to 4% of global turnover or €20 million for the most serious breaches.

Monitoring and Review

G Gaming reviews our practices and provisions on a regular basis to ensure that they reflect our commitment to ensuring fair, consistent and lawful management of data. This policy will be reviewed on at least an annual basis.

Linked work

No Links to display.

A.8.3 Media handling. Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.

A.8.3.1: Management of removable media

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:29

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 28/02/2022 at 19:51

What we do

Given the objective that most of our information is stored securely in the cloud to be accessed on authorised devices anywhere, there should be little need to transfer information using removable media.

Where removable media is necessary or practical it must be done in accordance with our defined policy (below).

Policy

The purpose of this policy is to define the rules by which removable media (e.g. a USB stick) may be used.

Policy Statements

Use of removable media must be in accordance with our:

1. [Handling of assets policy \(A.8.2.3\)](#);
2. [Terms & conditions of employment \(A.7.1.2\)](#);
3. [Acceptable use of assets policy \(A.8.1.3\)](#); and
4. [Code of Conduct](#).

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.8.3.2: Disposal of media

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:30

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 28/02/2022 at 20:09

What we do

At the end of the information management lifecycle, the secure disposal and/or reuse of media is critical to ensure accidental unauthorised disclosure or misuse of information and prevent a breach of confidentiality.

The policy below has been implemented to ensure the correct disposal procedures are followed.

Policy

This policy is designed to ensure information is protected from breaches in confidentiality through the correct erasure/decommissioning/destruction processes whenever it is to be reused or reaches its end of life.

Scope

This policy applies to any information bearing media used to collect, process, or store information of any classification higher than "Public".

This will include:

- Physical media:
 - Hardcopy materials - paper, etc
 - Magnetic media – removable hard drives, flash drives, USB sticks, etc
 - Electronic equipment:
 - Computers
 - Laptops
 - Mobile phones
 - Printers
 - Networking equipment etc.

Policy Statements

Hardcopy Media

- We are a paperless company with a remote team. Occasionally however some notes or print outs may result from our business operations. Paper waste classified above "Unclassified" should be shredded using a cross-cut shredder.

Magnetic media

- Data must be erased using approved secure-erasure software prior to re-use or disposal. Currently approved software is:
 - For Windows:

- [Eraser](#)
- [ATA Secure Erase](#) for solid state drives
- Mac OS:
 - [srm](#) command.
- Removable Hard Drives, USB Sticks, Flash drives – At end of life must be destroyed by an approved and certified organisation.

Note: where "Solid State" magnetic media is in use, approved erasure software must ensure that secure erasure is still possible. This is because solid state media is written to in a different manner than "spinning disc" media.

Use of Third-Party Secure Destruction Services

- Only certified and approved secure destruction suppliers may be used.
- A certificate of destruction must be provided by the service supplier.

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.8.3.3: Physical media transfer

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:30

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 28/02/2022 at 20:12

What we do

It is rare for employees to transfer physical media containing information. The most usual case of the transportation of physical media is when an employee is returning an asset or receiving one - in both cases

Confidential

the asset should be wiped before transport.

However, in the rare cases where physical media with information is transferred, it must be protected against unauthorised access, misuse or corruption during transportation. It includes physical media itself and devices which contain physical media, such as laptops when they are being transported without their regular user protecting them e.g. during repairs or other reasons.

General considerations

Only reputable, recognised brands and reliable couriers may be used for transporting physical media held on devices. Protection guarantees must be sought based on the classification of the information.

In accordance with our [Handling of assets policy \(A.8.2.3\)](#), "Confidential" or "Sensitive" information must be encrypted on the media on which they're stored, which provides a good level of protection in the event of theft or misplacement of the device.

Controls for two-factor authentication (2FA) oriented devices and media

- Hard token 2FA:
 - the 2FA device must not be stored or transferred with the device it unlocks (e.g. a case containing a laptop must not also contain the 2FA device); and
 - when a 2FA device is sent by post or courier it must not be sent in the same package as the device it unlocks.
- Soft token 2FA:
 - the 2FA processing device must not be the same device for processing information (e.g. the same smart phone) unless the device itself requires an unlock passcode that meets the standards of the [Mobile device policy \(A.6.2.1\)](#).

Lost device process

The following steps must be taken immediately:

1. An incident must be reported in accordance with the process for [Reporting information security events \(A.16.1.2\)](#);
2. An investigation carried out to establish:
 - a. What assets are contained on the media;
 - b. What protection of those assets is in place (e.g. encryption);
 - c. The likely party that now has possession the physical media;
3. Remedial action that may include;
 - a. De-authorising the device for any services that offer a remote reset and removal of access privileges.
 - b. Revoking any tokens on the device.
 - c. Changing affected passwords
 - d. A remote wipe of the whole device

Linked work

No Links to display.

A.9. Access Control

A.9.1 Business requirements of access control. Objective: To limit access to information and information processing facilities.

A.9.1.1: Access control policy

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:31

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 12/07/2022 at 15:56

What we do

G Gaming implements access control across its networks, IT systems and services in order to provide authorised, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Security Policy.

Access control systems are in place to protect the interests of all authorised users of G Gaming IT systems by providing a safe, secure, and accessible environment in which to work.

Scope

This policy covers all G Gaming networks, comms rooms, IT systems, data, and authorised users.

G Gaming's external website and other information classified as 'Public' is out of scope.

RESPONSIBILITIES

Members of G Gaming

All G Gaming staff, contractors and partners may have or require access to G Gaming data or IT systems and may be responsible for the systems upon which G Gaming's data resides.

System owners

Those with administrative control of systems (including designating access) upon which G Gaming data resides. This includes but is not limited to Google Apps, Quickbooks, Dropbox, and Slack.

Compliance officer

Responsible for writing this policy and establishing access control principles. Also responsible for the advising on and recommending information security policies to the Board, assessing information security risks, identifying, and implementing controls to risks.

Board

Responsible for reviewing information security policies.

POLICY

Principles

G Gaming will provide all employees, contractors and third parties with on-site access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

Generic identities

Generic or group IDs shall not normally be permitted as means of access to G Gaming data but may be granted under exceptional circumstances if sufficient other controls on access are in place.

Privileged accounts

The allocation of privilege rights (e.g. administrator, super-user) shall be restricted and controlled and not provided by default.

Authorisation for the use of such accounts shall only be provided explicitly and will be documented by the system owner.

Least privilege and need to know

Access rights will be accorded following the principles of least privilege and need to know.

Maintaining data security levels

Every user should understand the sensitivity of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user should still attempt to maintain the security of data commensurate to their sensitivity. The Data Classification Policy enables users to classify data appropriately and gives guidance on how to store it, irrespective of security mechanisms that may or may not be in place.

Users electing to place information on digital media or removable storage devices or maintaining a separate database are advised only do so where such an action is in accord with the information's security classification. Users are consequently responsible in such situations for ensuring that appropriate access to

the data are maintained in accord with the Information Security Policy and any other contractual obligations they may have to meet.

Users are obligated to report instances of non-compliance via Slack.

Instances of non-compliance will be published on G Gaming's risk register and supplied to external auditors upon request.

Access control authorisation

User accounts

Access to G Gaming resources and services will be given through the provision of a unique user account and complex password. Where possible, 2 Factor Authentication will also be enabled.

By default, staff are provided with access to Dropbox, Slack and Google Apps accounts.

By default, staff accounts will be suspended upon termination of contract, unless a request for an extension is received.

Access Management

1. Wherever and whenever access requirements change, this must be done through a formal process.
2. If an employee or other authorised person is suspended, their access must also be suspended.
3. When an employee or other authorised person leaves or ceases to work with the organisation, their access must be disabled in a timely manner.
4. Access will be audited on a scheduled, periodic basis.

Third parties

Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles.

The accounts will be removed at the end of the contract or when no longer required.

Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.

Passwords

Password issuing, strength requirements, changing and control will be managed through formal processes and in accordance with the guidance in the Information Security Policy. Every 3 months a password must be changed whether for google auth or more restricted systems.

Access to Confidential, Restricted and Internal Use information

Access to 'Confidential', 'Restricted' and 'Internal Use' information will be available to all members of G Gaming. Access to the systems and their data should be monitored by the System Owners.

There are no restrictions on the access to 'Public' information.

Policies and guidelines for use of accounts

Users are expected to become familiar with and abide by G Gaming's policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.

Access for remote users

Access for remote users will be provided in accordance with the Remote Working Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

Remote connections must use at least two-factor authentication to ensure the connection is secure and in line with the [Cryptographic Controls Policy \(A.10.1.1\)](#)

Access control methods

Access to data is variously and appropriately controlled according to the data classification levels described in the Data Classification Policy.

Access control methods include explicit logon to devices, Dropbox, Google Accounts and other methods as necessary. Where possible 2 Factor Authentication will be mandated.

Access control applies to all G Gaming-owned networks, servers, workstations, laptops, mobile devices, and services run on behalf of G Gaming.

Physical access control is documented in the [Physical Security Policy \(A.11.1.1\)](#)

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.9.1.2: Access to networks and network services

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:32

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2022 at 13:25

Covered in [A.9.1.1 Access Control Policy](#)

Linked work

No Links to display.

A.9.2 User access management. Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

A.9.2.1: User registration and de-registration

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:32

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 17:31

What we do

Registration and de-registration procedures are executed in accordance with our overall approach to access management as documented in our [Access Control Policy \(A.9.1.1\)](#).

For registration of new employees, this forms part of our onboarding for the employee.

For de-registration, this forms part of the Leaver's checklist which is triggered when an employee resigns or their contract is terminated.

Linked work

No Links to display.

A.9.2.2: User access provisioning

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:32

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 17:38

What we do

User access provisioning procedures are executed in accordance with our overall approach to access management as documented in our [Access Control Policy \(A.9.1.1\)](#) and is in accordance with the principles of:

- "Deny-by-default"
- "Need-to-know"
- "Least privilege"
- Role-based Access Control (RBAC)
- Information classification and the value of information assets

Initial user access provision comes with a minimal package: Dropbox, Slack, Google Accounts and may include coordination tools such as Airtable, leankit and trello.

Second level access is determined by the expected role type with differing packages of tools available to Developers, Account Management, DevOps, Finance and Artists.

Two factor authentication is mandated on all systems that enable it (including for google ID).

For registration of new employees, this forms part of the onboarding for the employee and is organised first by the employee's onboarding sponsor and then through a buddy system.

Privileged access rights require additional controls.

Linked work

No Links to display.

A.9.2.3: Management of privileged access rights

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:33

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 17:41

What we do

Procedures for the management of privileged access rights are executed in accordance with our overall approach to access management as documented in our [Access Control Policy \(A.9.1.1\)](#) and is in accordance with the principles of:

- "Deny-by-default"
- "Need-to-know"
- "Least privilege"
- Role-based Access Control (RBAC)
- Information classification and the value of information assets

Segregation of duties and segregation of privileged accounts from non-privileged accounts is implemented wherever possible and practical.

Special controls for access to particular Confidential systems are held only by Directors or for employees with specific requirements. Where possible, access to such systems is logged.

Linked work

No Links to display.

A.9.2.4: Management of secret authentication information of users

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:33

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 17:45

What we do

Procedures for the management of secret authentication information of users are executed in accordance with our overall approach to access management as documented in our [Access Control Policy \(A.9.1.1\)](#) and is in accordance with the principles of:

- "Deny-by-default"
- "Need-to-know"
- "Least privilege"
- Role-based Access Control (RBAC)
- Information classification and the value of information assets

The access control policy states that passwords must conform to complexity rules and must expire immediately after first use wherever possible.

Additionally, the requirement for users to keep such authentication information secret forms part of our [Acceptable use of assets policy \(A.8.1.3\)](#) and the sharing of such information is specifically identified as "unacceptable use" within the same policy.

Finally, two-factor authentication is used in all accounts, tools and systems where it is available.

Linked work

No Links to display.

A.9.2.5: Review of user access rights

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:34

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 18:18

What we do

The purpose of a regular review of user access rights is to reconcile who “should” have access (i.e. who is approved to have access) against who “actually” has access and what level of access they have.

Procedures for the review of user access are executed in accordance with our overall approach to access management as documented in our [Access Control Policy \(A.9.1.1\)](#).

Periodic review

An annual review of access rights will be conducted in accordance.

Review at change of access

Access rights are reviewed whenever a user joins, changes role within or leaves the organisation.

For new users this is done as part of their onboarding.

For leavers, this is done as part of the leaver's checklist.

Linked work

No Links to display.

A.9.2.6: Removal or adjustment of access rights

Assigned to: Natasha Mockett

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:34

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/03/2022 at 11:56

What we do

Procedures for the removal or adjustment of access rights are executed in accordance with our overall approach to access management as documented in our [Access Control Policy \(A.9.1.1\)](#) and is in accordance with the principles of:

- "Deny-by-default"
- "Need-to-know"
- "Least privilege"
- Role-based Access Control (RBAC)
- Information classification and the value of information assets

Removal of access rights

Access rights are removed on a timely basis determined with the following aspects in mind:

- Whether the termination or change is initiated by the employee, or external party, or by management and the reason of termination (e.g. good leaver or bad leaver);
- The current responsibilities of the employee, external party or any other user; and
- The value of the information and or assets currently accessible by the user and the position on the risk map for them.

A leaver's checklist goes over the access rights in place and when they should be revoked, then demonstrates they have been revoked at that time as described in [\(A.7.3.1\)](#).

The information and access rights that are removed or adapted include physical and logical access, keys, identification cards, information processing facilities, and subscriptions.

Change of authentication information following user exit

If a departing employee, or external party has known passwords for accounts remaining active, or codes for physical access etc, these are changed upon termination or change of employment, contract or agreement and communicated through the relevant channels.

Any user accounts and associated access credentials are revoked or rotated as appropriate as soon as an employee leaves who has previously had such access.

Linked work

No Links to display.

A.9.3 User Responsibilities. Objective: To make users accountable for safeguarding their authentication information.

A.9.3.1: Use of secret authentication information

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:34

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 18:24

What we do

Users have the responsibility for ensuring that secret authentication information remains confidential, including from other members of the organisation where that information relates to an account unique to them.

the requirement for users to keep such authentication information secret forms part of our [Acceptable use of assets policy \(A.8.1.3\)](#) and the sharing of such information is specifically identified as “unacceptable use” within the same policy.

Users understand their responsibilities and best practice with regards to Passwords and two factor authentication.

Linked work

No Links to display.

A.9.4 System and application access control

A.9.4.1: Information access restriction

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:35

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 18:46

What we do

Information access restriction is implemented in accordance with our overall approach to access management as documented in our [Access Control Policy \(A.9.1.1\)](#) and is in accordance with the principles of:

- “Deny-by-default”
- “Need-to-know”

- "Least privilege"
- Role-based Access Control (RBAC)
- Information classification and the value of information assets

Wherever possible applications are designed or selected such that menus do not show options for which a user is not authorised.

Applications are structured to ensure that 'open' access may be granted to defined areas - for example roadmaps or reports accessed by customers, while access to the whole application is restricted to employees and edit or oversight functions is restricted to key users.

Such read, write, delete, execute and approve rights are based on Role Based Access Control (RBAC) principles wherever possible.

Linked work

No Links to display.

A.9.4.2: Secure log-on procedures

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:35

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 22/02/2023 at 11:11

What we do

The use of secure log-on procedures is implemented in accordance with our [Access Control Policy \(A.9.1.1\)](#) which mandates that access is only granted through the use of individual usernames and passwords and multi-factor authentication when applicable and possible.

Access to mobile devices including the use of secure log-on mechanisms is documented in the "Technical Requirements" section of our [Mobile Device Policy \(A.6.2.1\)](#)

Logging of access attempts, successful or not, is implemented wherever possible and practical.

Linked work

No Links to display.

A.9.4.3: Password management system

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:36

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2022 at 13:28

Covered in **A.9.4.1 Access Policy and Access Restriction**

Linked work

No Links to display.

A.9.4.4: Use of privileged utility programmes

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:36

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 19:10

What we do

The controlled use of privileged utility programs is implemented in accordance with our [Access Control Policy \(A.9.1.1\)](#) and is in accordance with the principles of:

- “Deny-by-default”
- “Need-to-know”
- “Least privilege”
- Role-based Access Control (RBAC)
- Information classification and the value of information assets

Use of privileged utility programs is authorised on a “need-to-use” basis.

Furthermore, specific actions linked to the use of privileged utility programs are specified as “unacceptable” in our [Acceptable use of assets policy \(A.8.1.3\)](#) . Such activities include, but are not limited to:

- Effecting a security breach;
- Unauthorised port scanning;
- Unauthorised network monitoring and interception of data;
- Circumventing authentication mechanisms or other security controls; and
- Interfering with or denying service to other authorised users.

Linked work

No Links to display.

A.9.4.5: Access control to programme source code

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:36

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 23:09

What we do

Access to programme source code is implemented in accordance with our [Access Control Policy \(A.9.1.1\)](#).

Each user's access is controlled and fully logged and auditable. Access to Production environments and systems are even more closely controlled through restriction to a very small number of named users with access logs.

Linked work

No Links to display.

A.10. Cryptography

A.10.1 Cryptographic controls. Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.10.1.1: Policy on the use of cryptographic controls

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:37

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 11/01/2023 at 11:12

What we do

G is committed to ensuring that employees are aware of their responsibilities in relation to the Company's cryptographic controls. The policy below is designed to ensure that cryptographic controls (i.e. the use of encryption technologies) is applied in a consistent, adequate and proportionate manner and that key material is formally managed.

Policy

The purpose of this policy is to protect the confidentiality, integrity and availability of the organisation's Information by applying appropriate levels of Cryptographic control.

It is necessary for all employees, contractors, agents or other workers, hereinafter collectively known for the purposes of this policy as employees, to understand the Company's policies and how they apply.

Policy Statements

General principles

1. All critical or sensitive data transferred outside of the organisation must be encrypted.
2. All removable media, including memory sticks, must be encrypted.
3. Laptop hard drives must be encrypted.
4. All remote access must take place via encrypted terminal or VPN services.
5. Wi-Fi Protected Access encryption is mandatory for all wireless networks carrying organisational data (including domestic networks where remote working is undertaken).
6. Where available SFTP must be used for file transfer.
7. If SFTP is not available, FTP may be considered, but it is highly recommended that this only be used for information classified as "Public". If more valuable information is to be transferred and FTP is the only method for doing this, the risks must be identified, evaluated and accepted by the risk owner prior to use"

Confidential data should never be included in the body of an email message. If an employee must send confidential data, it must be sent as an attachment and the file should be encrypted prior to attaching in order to prevent unauthorised disclosure of sensitive data, including data such as player data or data relating to winning information. Note that this does not include the result of a round sent to Operators to confirm the legitimacy of a win since no personally identifiable player data should be included in such information. The decryption key should be provided to the recipient via another separate method of transmission. Because many email filters will block emails that have an encrypted file attached, the company provides a secure file transfer application for sending sensitive data via Dropbox.

Encryption of data in transit

1. Data classified as "Confidential" must be encrypted in transit.
2. Data classified as "Private" should be encrypted wherever possible and practical.
3. Data classified as "Public" or "Open" may be sent unencrypted.

Key management

The company uses the following measures to protect encryption keys:

1. An accessible copy of the encrypted data should be kept in case the encryption key is lost or forgotten. This may be achieved by maintaining an accessible copy of the data on a company-managed server or using an enterprise encryption solution that provides an authorised systems administrator access to the data in the event of a lost or forgotten key
2. Encryption keys should be protected with a strong password
3. Encryption keys that are used to protect sensitive data are themselves to be considered restricted data
4. All encryption passwords should be kept confidential and not shared with others
5. All encryption passwords used to access encrypted devices must never be stored on, near or with the encrypted device
6. Rules relating to encryption on removable media are contained within the [Management of removable media policy \(A.8.3.1\)](#)

7. The strength of encryption to be used must be considered against the risks associated with the assets to be encrypted. As a guide, a minimum of 1024 bit encryption is strongly recommended.
8. Some technologies for VPN or SSL/TLS use AES 256-bit encryption and this is viewed as sufficiently secure.

Roles and responsibilities

1. Ensuring that the organisation maintains the highest practicable standard of encryption is the responsibility of the CTO
2. Key management responsibility lies with the IT administrators.
3. All individuals are responsible for ensuring that “Sensitive” data is encrypted before leaving the organisation's premises.

Regulation of cryptographic controls

For any use of cryptographic controls exported outside of the UK the following considerations are made:

1. Regulatory controls for any country to which data is exported outside the UK must be checked to ensure that cryptographic legislation will not be contravened.
2. Restrictions on import and/or export of computer hardware and software for performing cryptographic functions (e.g. under the [Wassenaar Arrangement](#) for export controls for conventional arms and dual-use goods and technologies);
3. Restrictions on import and/or export of computer hardware and software which is designed to have cryptographic functions added to it;
4. Restrictions on the usage of encryption; and
5. Mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.10.1.2: Key management

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:38

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/03/2022 at 12:03

What we do

Key repository

Public keys for persons accessing our services are managed within a key repository - Github. The passwords which allow access to this are stored within the organisation's secure password manager. All modifications to public keys are traceable.

Access to this repository will initially be limited to the organisation's technical employees. The CTO is responsible for the maintenance of the repository to preserve integrity of the key information. As such the CTO will be responsible for reviewing changes to the repository. Changes to the keys are auditable.

Key addition

- request made to add key;
- CTO verifies that key meets the key specification;
- if key meets specification then the key is added to the key repository;
- if key does not meet specification then the requester must provide a key which does meet specification.

Key revocation

- owner of key being revoked advises CTO;
- CTO marks key as revoked and removes key from all services;
- owner supplies CTO with new key;
- CTO adds new key to the authoritative key records;
- CTO ensures that all services use the new public key.

Key removal

- request made to CTO to remove key;
- CTO removes key from repository.

Key specifications

The key must be of the type RSA and be 2048 bits. The private key must have a passphrase which at least conforms to the minimum requirements for passwords

Key backup

Keys are stored in Github, meaning there is always access.

Linked work

No Links to display.

A.11. Physical and Environmental Security

A.11.1 Secure areas. Objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

A.11.1.1: Physical security perimeter

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:40

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 01/03/2022 at 15:45

What we do

Areas to consider physical security

We have three types of property from which to consider physical security. These are:

1. Data centres that host our information assets
2. Workers who spend a large proportion of their time remotely at home
3. Workers who do predominantly 2 but also use co-working spaces, hotels, customer's premises etc

As a modern business we keep the majority of information assets in the cloud, secured within established and ISO 27001 certified data centres, using well protected applications and services like ISMS.online and other recognised brands.

Data Centres

The risks around physical security of those selected data centres is transferred to all data centre providers we use separately holding their own 27001:2013 certificate or other standards that are equal or better.

We gain assurance through our controls for [Supplier Relationships \(A.15\)](#)

Home and remote workers

As a remote-working organisation, some physical security policies and processes apply at home.

Staff should:

- Have appropriate security standards in their homes and perimeters as would be needed for achieving home and contents insurance from a reputable provider (e.g. locks on doors and windows)
- Work in a quiet place without distraction from other family members
- Secure their devices in accordance with the policies for informational processing facilities (if a director then also backup the device locally too)
- Protect their network and router access using standards expressed in this ISMS
- Keep the clear desk and clear screen policy enforced as though it were an office at work in accordance with the wider ISMS
- "Confidential" or "Sensitive" documents must be secured away from other home users' access

Employees who use other premises

Other parts of the ISMS address security of equipment off premises and in addition to that the following points apply when working from other premises such as co-working spaces, hotels, cafes, trains, customer offices, and supplier premises:

- The device screen, or paper materials, should be positioned so it can't be read by unauthorised people (e.g. sit with your back to the wall away from others in a café).
- Use of Wi-Fi in public premises must only take place if:
 - a personal hotspot or company provided Wi-Fi is not offering a good connection; and
 - if the Wi-Fi offers secure access to the standard expressed in this ISMS. Any connection to public Wi-Fi must be for the shortest possible time and avoid transmission of anything such as financial or sensitive information.
- Private VPN for access on the move is encouraged if no 3G/4G personal Wi-Fi/hotspot is available and communication is urgent.
- Work assets such as laptops must not ordinarily be left in rooms or vehicles unattended. In instances where they need to be (e.g. attending an evening function and staying in a hotel) the asset must be hidden and normal ISMS precautions taken.

Linked work

No Links to display.

A.11.1.2: Physical entry controls

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:40

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 08:40

G is a fully remote company without permanent physical offices. We expect the physical controls of lockable doors and windows that are standard to an employee's home to be sufficient.

Our key third party suppliers - such as AWS or Gibtel, are ISO27001 certified and thus have appropriate controls.

Linked work

No Links to display.

A.11.1.3: Securing offices, rooms and facilities

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:42

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2022 at 13:00

G is a fully remote company, however, we expect employees to use standard security measures in their own homes. These are explained in our A.8 Asset Management Policies and in our A.11 Physical and Environmental Security Policies.

In general, employees should use sensible security measures:

- Do not leave laptops or other equipment or any sensitive data visible when you are not physically present in the room for an extended period of time

- Make sure your house has up-to-date locks on windows and doors and an alarm system if possible which is used when out of the house.
- Do not leave a laptop unattended when in coworking spaces, cafes or while travelling or in customer or supplier premises.
- If leaving a laptop or notebook, ensure that it is password protected and with screenlock activated as per our Mobile working and Acceptable Use policies.

Linked work

No Links to display.

A.11.1.4: Protecting against external and environmental threats

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:45

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 08:45

As a fully remote office, our general rules of standard security are sufficient to cover the likely external and environmental threats in an employees home or co-working space. These include sensible and normal measures such as employees would use as part of their daily life including for security and safety.

Do Not leave your laptop unattended. Be careful of your own safety in the case of any confrontation or direct risk. Be aware that conversations can be overheard as well as documents being read on an open laptop.

Linked work

No Links to display.

A.11.1.5: Working in secure areas

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:47

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2022 at 13:11

G does not have physical offices and regards employee homes as sufficiently secure (when following the various policies and advice laid out in these policies). Employees working in co-working spaces need to think differently about security as laid out in A.11.1.1.

However, when thinking about the security of our informational file structure and the resulting confidentiality of any data produced (from documents to code) or any data collected (from player data to game transaction data), employees should consider our Data Management and handling Policy and Data classification. The need to keep company information held in a secure area is one reason for a policy of not storing any files locally, but instead relying upon the additional security from third party storage which is backed up and less vulnerable to loss or damage.

Linked work

No Links to display.

A.11.1.6: Delivery and loading areas

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:47

Statement of Applicability: Not Applicable This control has been identified as “Not Applicable” and is not relevant to the scope of the ISMS. This has been confirmed through risk assessment.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2022 at 13:30

G has no physical offices and as such has no delivery or loading areas. Should staff be taking or organising deliveries of company equipment or information at home, they should be mindful of standard security procedures, including using only reputable, tracked courier or delivery companies and requiring signature and tracking information for parcels and letters.

Linked work

No Links to display.

A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.

A.11.2.1: Equipment siting and protection

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:49

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 08:48

What we do

As a fully remote company, we expect employees to take basic physical security measures around their devices, including:

- Information processing facilities (laptops, desktop machines etc) handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorised persons - including friends and family at home.
- Staff must keep food and drink away from ICT equipment.
- Devices must not be left unattended and should be transported correctly (ie with appropriate protection to avoid damage in transit and to minimise the risk of theft)
- Any multi-factor authentication to allow access to the devices must be stored separately from the device itself when not in use.

Linked work

No Links to display.

A.11.2.2: Supporting utilities

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:49

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 19:34

What we do

The organisation predominantly uses cloud-based services from large, well-established providers, who are responsible for provision of assured utilities within their respective datacentres.

Contingencies for telecommunications and internet services at offices and home offices include the use of mobile networks, dongles and personal hotspots within the context of other relevant ISMS controls.

Linked work

No Links to display.

A.11.2.3: Cabling security

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:49

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 19:36

What we do

The organisation uses cloud-based services from large, well-established providers, who are responsible for cabling security within their respective datacentres.

Our assurance relating to cabling security for both of the above is managed through controls relating to [Supplier relationships \(A.15\)](#).

Linked work

No Links to display.

A.11.2.4: Equipment maintenance

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:50

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2022 at 13:16

What we do

The majority of our equipment falls into two categories:

Equipment covered by large, well-established providers, who are responsible for provision of assured utilities within their respective datacentres and who's reliability and maintenance is covered by the relevant Service Level Agreements in place via our Supplier Contracts.

Personal devices such as laptops and mobile devices. In the event the equipment needs to be repaired, then the repairer must be a recognised provider of repair services for that type of device, e.g.: Apple Store, PC World etc. where we tolerate the risk based on the controls used by those companies.

They must also provide suitable receipts and advice notes for our records which are kept by the employee before passing over to the finance team for record keeping.

In the event that staff owned device, such as a mobile phone, used to access organisation information (e.g. e-mail) requires repair, all passwords for services accessed from that device must be changed before submitting the device for repair. They must only be re-input once the device has been confirmed working and tamper free.

Note - staff must not leave valuable information on local devices as the sole point of failure and all business-critical information must reside on the designated cloud service.

Maintenance is expected to be minor and includes simple best practice such as regularly cleaning a laptop or mobile screen and keyboard. Preventative measures are encouraged such as using a screen protector, a case and a sensible travel bag that offers protection against accidental damage.

Linked work

No Links to display.

A.11.2.5: Removal of assets

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:50

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2022 at 13:19

Our only removable equipment is covered by our Mobile Working Policy. If employees do need to use any device that involves creating local copies of company assets (such as storing data on a removable hard-drive), then they should remember to back up the information onto a shared drive at the earliest opportunity and to maintain sensible security standards towards the removable asset just as they would to a company laptop or mobile device as per our Mobile Working and Acceptable Use policies.

Linked work

No Links to display.

A.11.2.6: Security of equipment and assets off-premises

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:50

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 20:18

What we do

G is a fully remote organisation and thus employees are responsible for their own equipment.

The following security precautions apply to organisation owned assets and assets owned privately used on behalf of the organisation e.g. BYOD mobile devices:

- Mobile device controls as per [Mobile device policy \(A.6.2.1\)](#)
- Home working and teleworking controls are as per [Teleworking \(A.6.2.2\)](#)
- The organisation has adequate insurance cover to protect equipment off-site however in the event of negligence or incompetence by the member of staff, they will be responsible for the replacement of the equipment and may be subject to investigation and the [Disciplinary process \(A.7.2.3\)](#).
- When equipment is transferred between members of staff a record of that transfer must be made against that item within asset register if permanent.

Linked work

No Links to display.

A.11.2.7: Secure disposal or reuse of equipment

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:51

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 20:21

What we do

Our policy on secure disposal or reuse of equipment is contained within the policy for [Disposal of media \(A.8.3.2\)](#).

Linked work

No Links to display.

A.11.2.8: Unattended user equipment

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:51

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 20:24

What we do

Security precautions relating to mobile devices are covered in our [Mobile device policy \(A.6.2.1\)](#).

Other controls are covered in our [Clear desk and clear screen policy \(A.11.2.9\)](#).

Awareness relating to unattended using equipment is contained within our [Information security awareness, education and training \(A.7.2.2\)](#).

Linked work

No Links to display.

A.11.2.9: Clear desk and clear screen policy

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:51

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 02/03/2022 at 20:41

What we do

At G Gaming we have a clear screen policy. As a fully remote company, a clear desk policy is not relevant, although of course employees must take into account any sensitive printed material left around their desks even at home and must follow sensible precautions when in public spaces as detailed in our Mobile and Teleworking Policies.

This takes into account:

- [Classification of information \(A.8.2.1\)](#); and
 - [Identification of applicable legislation and contractual requirements \(A.18.1.1\)](#)
-

Policy Statements – Clear Screen

1. Devices must have a lock screen enabled.
2. There is no need to physically secure devices as long as the room in which the device is held has adequate security (e.g. door locks, or it is within trusted premises).
3. If there is any concern for safety, then employees must take their device with them.
4. If users are working where they may be overlooked by unauthorised parties, then they must either:
 - a. Move such that they cannot be overlooked;
5. apply a “privacy screen” to the device; or
6. Ensure they are working on “Public” or “Open” information and no higher in classification.

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.12. Operations Security

A.12.1 Operational procedures and responsibilities. Objective: To ensure correct and secure operations of information processing facilities.

A.12.1.1: Documented operating procedures

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 08/03/2023

Status: Completed

Approved by Helen Walton on 08/05/2024 08:53

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/03/2022 at 12:10

What we do

We are an organisation that primarily uses cloud-based applications and systems, so many traditional operations such as computer start-up and shutdown, backup etc are not relevant – or at least the responsibility of the service provider.

Our assurance relating to operational procedures within the above is managed through controls relating to [Supplier relationships \(A.15\)](#).

Beyond our use of third-party providers, contained within this ISMS are a number of processes related to Information Security including:

- [Equipment maintenance \(A.11.2.4\)](#)
- [Change management \(A.12.1.2\)](#)
- [Capacity management \(A.12.1.3\)](#)
- [Controls against malware \(A.12.2.1\)](#)
- [Information backup \(A.12.3.1\)](#)
- [Logging & monitoring \(A.12.4\)](#)
- [Installation of software on operational systems \(A.12.5.1\)](#)
- [Technical vulnerability management \(A.12.6\)](#)

Our main repositories for documented operating procedures is:

- *Dropbox (policies and procedures)*
- *Swaggerhub (integration)*
- *Notion (internal wiki)*

- *Github - (code standards)*
- *Freshservice - customer support tickets and incidents*

Documented Procedures include:

Product Development

- *Planning - how to manage product development*
- *Compliance - how to plan and manage the game certification process*
- *Development Testing, Change Management and Release*
- *Translations*
- *Bet Configuration*
- *RTP Testing*
- *Gitlab Repositories*

Integrations and systems

- *Integration with GPAPI; Integrating with an Operator*
- *Network and System Configuration and Maintenance*
- *System, Health and Performance Monitoring*
- *Access Control*
- *Infrastructure Mapping*
- *Alerting*

Finance and Business Planning

- *Finance and Accounting Management Practices*
- *Business Continuity Planning*
- *Business Reporting*
- *Recruitment and Staff Onboarding*
- *Leavers Process*
- *Corporate Structure*
- *Financial Reporting in all guises*
- *Due Diligence*
- *Employee Card Management*
- *Subscription and Expense Management*

Customer Service

- *Win Checks and Player reviews*
- *Support/Rota/BAU*

- *Billing*

Sales, Marketing and Accounts

- *Incident Handling and Reporting*
- *Rolling out Products*
- *Promotions*
- *Onboarding Customers*
- *Social Media and Website*
- *Event Planning*
- *Account Management*

Linked work

No Links to display.

A.12.1.2: Change management

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:56

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 08:56

What we do

Gamevy takes a risk-based approach to all our Change Control Process.

As part of this we aim to understand our baseline, log any changes against that, and accurately classify each change against relevant criteria to enable the team to manage each change appropriately and within the relevant guidelines.

As part of our regulatory compliance, we now review the log quarterly, and hold an annual review not only on the log and the process, but also on our policy.

The Baseline

1. Component asset register

Gamevy's gaming system is made up of a series of inter-related hardware and software components relating to the platform, RNG and games. These are recorded and defined within the Component Asset Register. Each entry must confirm to the following requirements:

- Definition of the component
- Unique identification number
- Version number
- Identifying characteristics
- Component owner (responsible person)
- Classification (related to confidentiality, Integrity, Availability, Accountability)
- Checksum / hash value for components classified as '3 – substantial relevance'
- The geographical location if the component is a hardware / virtualised component
- Classification of components

Each of the components identified within the register is categorised using a 'relevance' code defined against 4 criteria:

- No relevance (the component can have no negative impact on criteria)
- Some relevance (the component can have an impact on criteria)
- Substantial relevance (the criteria is related to or directly dependent on the component)

The criteria are:

- **Confidentiality** – confidential information regarding the customer (PII / transactional information)
- **Integrity** – the integrity of the system, its functionality and the information stored in the system
- **Availability** – the availability of information concerning the customer
- **Accountability** – user activity (including customers / personnel / 3rd parties) in relation to the component
- Assigning a relevance code

Each component is assessed against the criteria above and the highest individual code is assigned to the component overall.

Example: '7UP-CF-03' (the payable critical file of the game 7-Up, is given the following criteria codes:

- Confidentiality – 1
- Integrity – 3
- Availability – 2
- Accountability – 3

In the above example, the highest code is '3 – substantial relevance' assigned against both Integrity and Accountability, since the payable will impact on the amount paid to a customer, the game's overall fairness and the game payout's relation to the published rules.

Changes to games and systems are often necessary due to customer requests, market evolution or business pressures. Yet since any change to our games, systems or platform could impact on customers and also impact on our regulatory compliance, all changes must be logged in order not only that we are aware of potential impacts, but also that we can audit them regularly.

1. As a minimum each material change includes:
2. A description of the change
3. A classification of the change (complexity / resourcing etc)
4. Categorisation (based on relevance code)
5. Status of the change
6. Approvals covering the lifetime of the change
7. A description of how the change will be implemented
8. A justification outlining why the change is needed
9. A risk assessment of the change / impact evaluation

Change Management Approvals

As a small and agile company, our approvals process should walk a line between being sufficiently light-weight to be fit for purpose and sufficiently rigorous to meet regulatory expectations. Where possible automated software, logging and auditing will be used to assist in this.

However, as a minimum, for each stage, approvals and 'action items' must have time / date, name and responsibility logged.

Changes with a relevance code of 1

No approval required from the accredited testing organisation. All changes still need to be logged and follow change management processes.

Changes with a relevance code of 2

Requires submission to an accredited testing organisation on a quarterly basis.

Changes with a relevance code of 3

Requires pre-assessment by the accredited testing organisation, and approval prior to making changes. These changes must also be included in the quarterly reporting process for relevance code 2 changes.

Regulatory approvals and reporting

We take especial note of the following key areas where prior approval is required:

- RNG – implementation of new RNG and / or changes to existing RNG shall be notified 5 days before implementation or changes is carried out
- Changes to existing games which affect the use of Standard Records, must be notified 5 days before implementation. Examples of Standard Records must be submitted along with the notification

- Situations where the regulator's Standard Records cannot be used – 60day advanced notification required. Development will not commence until approval has been granted.

The following key areas do not require exceptional prior approval :

- Implementation of new games – new games which do not affect how the regulator's Standard Records are used can commence without prior approval
- Changes to existing games – where the use of regulator's Standard Records does not change, no prior approval is required

Reporting

If they are requested either by our regulator or our accredited testing organisation. or as part of an internal review process, we shall always have available:

- Component register
- Change history of an individual component
- Geographical location of all hardware / virtual servers
- A report on all verified changes

Each quarter a change log shall be examined by our third-party testing house. Each year, an audit will establish a new baseline and a re-certification process will be carried out.

Differing regulators and operators have alternative systems. For example, Loto Quebec uses a similar change management weighting system, but requires changes to be made via their proprietary platform reporting system. They also check SHAs daily to ensure the game served is identical to the one originally certified. These alternative reporting systems conform to the principles described in this policy but are mapped in our customer and jurisdiction specific procedures/checklists.

This policy is supplemented by our wider development change management and release development standards - key process considerations are below.

Roles & Responsibilities

The following table identifies the Roles & Responsibilities relating to Change Management.

Role Name	Role/Responsibility/Authority
Board Members	• Ensure that the necessary information security controls are implemented and complied with as per this policy.
CTO	• Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries; • Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards; • Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products;

	• Co-ordinate the overall communication and awareness strategy for change management; • Acts as the management champion for change management and control; • Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable. • Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives; and • Co-ordinate the implementation of new or additional security controls for change management.
Development Team leads	• Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders; • Approve and authorise change management and control measures on behalf of the organisation; • Ensure that all team members are aware of the applicable policies, standards, procedures and guidelines for change management and control; • Ensure that policy, standards and procedural changes are communicated throughout the team; • Report and evaluate changes to change management and control policies and standards; • Co-ordinate the overall communication and awareness strategy for change management and control; • Co-ordinate the implementation of new or additional security controls for change management and control; • Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified; • Provide regular updates on change management and control initiatives and the suitable application; • Evaluate and recommend changes to change management/version control solutions; • Co-ordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company. • Establish and implement the necessary standards and procedures that conform to the Information Security policy; • Responsible for approving, authorising, monitoring and enforcing change management initiatives and related security controls within all companies and divisions; • Ensure the compliance to this policy and report deviations to the CTO.
IT Service Providers	• Shall comply with all change management and control statements of this policy.
Developers	• Shall comply with all information security policies, standards and procedures for change management and control.

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Development Process Considerations

Mirrored Production Environment

Software development is carried out on a local machine and uses virtualisation technologies which enable a near-mirror of the production environment to be hosted locally. This means that when creating any changes, the developers run tests on their own machines in the virtual environment. The behaviours of the production environment are mocked in order to represent the live system and its interactions with third parties as closely as possible.

Full Automated Testing

As software development is carried out, a number of types of automated tests are created to provide feedback. Unit Tests are the most granular and exist to verify that individual functions perform as intended. Integration Tests are at the next layer. They work to verify the function of a logical grouping of code. End-to-End tests pass all the way through the system. They mimic the behaviour of the game and so provide absolute confidence in key aspects of the software such as in the placing of bets. Because of the nature of the applications that G is producing – iOS and Android applications – client-side testing is difficult. However, when it can be achieved, Client Side tests are used to test core features such as the sign up, account management and transaction history functions.

Branching

All software development is carried out on a feature-branch. This means that changes are isolated from the main branch of production code. The changes made on a branch can be tested in isolation, and any changes to configuration are easily identified. A branching policy allows for changes to be collated and described as a Changeset. It also allows for manual review, detailed below. Finally, it ensures that any changes can be rolled back almost instantaneously should we encounter problems.

Change Control Authorisations

All software written at G is stored in source control. Source control allows for any change to be traced back to an individual. This is further reinforced by the practice of Manual Code Review, meaning that no change can be merged into the master branch without an independent developer reviewing and authorising the change. The independent developer, who takes co-responsibility for the change and whose review steps and comments are recorded, can also be traced.

Code understanding and Change Documentation

Developers must understand the codebase if they are to make changes with confidence. Traditional documentation tends to become obsolete very quickly and is insufficiently dynamic or responsive to changes. G is a leading exponent of full, dynamic documentation via automated tests.

Especially important to this are automated acceptance tests which describe the expected functionality and assumptions inherent in the code. The tests protect against future changes which may break dependent code, as well as offering an in-depth and up-to-date understanding of the codebase for new employees or those auditing the code.

Manual Code Review and Sign Off

This step is a cornerstone of our change release and formal integration process. It ensures that code which is merged into the main branch conforms to G's standards, and that no suspicious or malicious code can be introduced. The developer who authors the software for a new feature or game is restricted from being able to merge that code into the main branch.

When code is merged back into the master branch, a procedure which formally accepts the new feature / game is followed, using an independent developer who follows a series of review steps. In addition the person who requested the development of the feature or game, or whoever took overall responsibility for it, reviews the changes before deciding whether development can be signed off. Part of this review includes a check of whether a 3rd Party Testing house needs to be involved. Records of this process, including any feedback is held in Github and also integrated to the team messaging platform.

Release Controls

Though all of G's releases are automated in terms of the mechanics of how they occur, the release to a production environment is triggered by an individual taking an action within our build management system, Jenkins.

Low Risk - where the release risk has been quantified as Low, it can be performed following G's standard continuous deployment methods. That means it can occur at any time and can be unattended - it relies on a comprehensive suites of automated tests rather than any human intervention.

Medium Risk - where releases are deemed to be of Medium risk, the release is timed to occur during business hours so that they can be live-monitored by the people implementing the change.

High Risk - for a release that contains a high degree of risk, the team set aside an agreed Maintenance Window during which the release will be made. This will be planned in advance for a particular time. Customers are informed of the Maintenance Window, and no play is allowed during that time. This permits G to monitor a release in absolute safety in a live environment before introducing real customers.

In due course for both medium and high risk releases, G plans to begin blue/green releasing, whereby two versions of the software are kept running side-by-side. Customers are switched over to the new version in batches, allowing G to gradually increase the load on the new version until all customers have been moved over.

Risk Review

Risk assessments occasionally suffer from a well-known problem. Because they call for subjective judgements, they are not always reliable and can even be deliberately misapplied in order to make a release easier or subject to fewer controls. G defends against these problems by a process of review. Just as no developer can merge code into the master branch without an independent review, no release can be performed without an independent person reviewing its details and signing it off.

Monitoring

Monitoring of the production system ensures that after a release has taken place, any problems that occur can be identified before they affect customers. A set of key metrics are monitored and compared against known baselines to identify any trends suggestive of problems. At pre-arranged trigger points a notification is sent to the developers involved who investigate and take action accordingly. For medium risk releases, developers are expected to be monitoring the system in person.

Maintenance Windows

When a Maintenance Window is necessary, the fact is advertised to customers in advance. A maintenance window will be advertised for a minimum of 24 hours within the client application. So as to minimise the

amount of customers exposed to maintenance window, data of off-peak times will be used to plan them for the periods of lowest play.

At the point a maintenance window begins, all current play is allowed to end. Where necessary, customer will be barred from gambling further during the allotted period of time.

Linked work

No Links to display.

A.12.1.3: Capacity management

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:57

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/03/2022 at 12:07

What we do

As an organisation that primarily uses cloud-based technologies, we are able to rapidly increase capacity as required. On our standard system, we also have automated capacity increases - when the disc measures close to capacity, it autoscales to increase available capacity.

We forecast capacity requirements and load across our endpoint locations with DevOps engineers working closely with Account and Sales managers to forecast customer demand, especially for high demand times caused by marketing activity or launches. This is supplemented by automated forecasting via our monitoring systems which enable planned increase in capacity with emergency auto-scaling as a failsafe.

We monitor capacity usage using a variety of tools which include automated alerting to warn of system problems for a fast response.

Linked work

No Links to display.

A.12.1.4: Separation of development, testing and operational environments

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:57

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 18:46

What we do

G Gaming has three environments and the same baseline system is used on all three environments: development, staging and production.

- Development – for development and internal testing
- Staging - for full testing before release which also can allow customers and other stakeholders including third party testing partners to test the games
- Production environment – the live operational environment containing multiple customer “instances” of the platform.

Linked work

No Links to display.

A.12.2 Protection from malware. Objective: To ensure that information and information processing facilities are protected from malware.

A.12.2.1: Controls against malware

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:58

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 17:18

What we do

We empower users by giving the freedom to access external information online without restriction or lockdown of sites as long as they stay within the boundaries of our:

- [Terms and conditions of employment \(A.7.1.2\)](#);
- [Code of conduct](#); and
- [Acceptable use of assets policy \(A.8.1.3\)](#)

We also encourage them to stay abreast of general security best-practice procedures and precautions. Staff communications and awareness on the subject is also assured through our Slack and Notion pages as well as [Information security awareness, training and education \(A.7.2.2\)](#). Given these controls and those below we do not employ any other explicit form of software whitelisting or blacklisting.

Deliberate actions taken by users to deactivate anti-malware controls (e.g. anti-virus software) is specifically noted as "Unacceptable use" in our [Acceptable use of assets policy \(A.8.1.3\)](#) and may lead to investigation and possible use of the [Disciplinary Process \(A.7.2.3\)](#).

For devices used by employees;

The use of anti-virus software on employee devices detects and eliminates the vast majority of common malware that is in existence.

We use well-known and widely trusted products to minimise the risk that a user will encounter malware.

This is supported by our [Mobile device policy \(A.6.2.1\)](#).

For our online services

- Document uploads are scanned for viruses daily.
- Protection against malicious user input: SQL injection, XSS, CSRF and mass assignment.

Malware in documents

Documents may contain malware in the form of macros, for example macros in Word or Excel documents. Caution must be exercised when opening documents that contain macros. We need to check that the received document:

- Is sent by a known or trusted source;
- Is expected or is likely to be something that the sender would normally send out (i.e. the sender's computer hasn't been compromised by malware which sends out infected documents).

The decision to open the document must be based on these criteria. Where there is doubt the recipient must contact the sender of the document to obtain confirmation before opening the file.

Anti-malware requirements

In all cases where anti-malware software is installed:

- The software must be regularly updated using the auto-update feature of the software;
- Malware scanning must occur when files are accessed.

For users running Windows the following must be in place and active:

- Anti-virus software which scans email that is processed by the device;
- Software firewall (the standard Windows 7 firewall or higher is adequate);
- Regular updates to the OS, but not so often that it hampers productivity.

For users running Mac OS X the following must be in place and active:

- Software firewall (the standard Mac firewall is adequate);
- Regular updates to the OS.

For users running Linux the following must be in place and active:

- Software firewall;
- OS updates at the discretion of the user.

Software firewall configuration:

- Must be configured to block all incoming connections with allowed connections being specified on a white-list basis or to interactively prompt the user to permit/deny incoming connections.

Suspected or actual compromise

If a user suspects or has actually been infected by malware (including viruses, worms, trojans etc.) they must immediately shut down the laptop and raise a security event as per [Reporting information security events \(A.16.1.2\)](#).

Linked work

No Links to display.

A.12.3 Backup. Objective: To protect against loss of data.

A.12.3.1: Information backup

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 08:59

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 17:53

What we do

Customer information gathered in the course of delivering the games G Games publishes is recognised as of vital importance.

All of the data stored in G Games's database is backed up in two ways:

- It is replicated in real time to another completely redundant slave server.
- Snapshots of the data are also taken on an hourly basis.

These backups are shipped to a file store in a separate location to where the data centre is located so that in the event of catastrophic failure, a recovery can be performed.

Security

The source code itself relating to G Games' application and services is held in secure, distributed version control repositories provided by GitHub. This global service is fully distributed, meaning it offers continuity of service and has its own highly robust back-up system, making it an exceptionally low-risk choice.

Though GitHub is the central source of a repository, a local copy including a full history of the changes made is also stored on each of the developer's machines. This offers an emergency back-up fail-safe, and its security is managed via the measures described elsewhere in this policy.

Back Up Standard

- Automated backup systems shall be used to perform scheduled system backups of target data to ensure that data are consistently available to conduct business and support business operations.
- All sensitive and critical data shall be stored on network servers or cloud-based services so that they may be backed up on a regular basis.
- Full backups shall be performed at least weekly.
- Incremental backups shall be performed at least daily.
- Backups and associated media shall be retained for disaster recovery purposes.
- Backup media shall always be:
 - Encrypted when sent offsite
 - Secured while onsite
 - Kept in locked containers when transported to/from the offsite facility
 - Transported using a trackable courier service

- Full back up media shall be stored at an approved off-site facility.
- Only authorized personnel shall have the ability to recall storage media from offsite storage.
- Backup inventories shall be maintained for all backup media.
- Restore testing shall occur on a quarterly basis to test the ability to restore from backup media. Testing must be logged.
- Backup logs shall be kept indicating the success or failure of the backup and shall be retained for at least one year.
- Backup job detail reports shall be retained for at least one year.
- Backup job descriptions shall be retained for at least one year.
- If a backup does not complete successfully within a 24-hour period, a notification alert shall be automatically sent.
 - Processes for managing failed or incomplete backups must be documented.
 - Documentation for failed or incomplete backups must be maintained for the audit period.
- Backup media that are identified as unusable or damaged shall be securely shipped for certifiable destruction.

Database Replication and Failover

Setup

If the config for that environment includes a replica:

```
{  
  
"target_environment": "prod",  
  
"app_server_count": 2,  
  
"database_primary_server_count": 1,  
  
"database_replica_server_count": 1,  
  
"monitoring_server_count": 1  
}
```

then running the main playbook is enough to prepare the servers. Once this is complete the setup_replication script needs to be run; this copies the data from the primary and enables the replica as a hot standby (read-only).

Failover

If there is a problem with the primary, then the failover script should be run. This will promote the replica (allowing writes) and update the bornlucky config files to point at the new primary.

Once this is complete, the replica server needs to be renamed as a primary, before the main playbook is run again. If the old primary still exists, then it should be deleted as well. As long as the server has been renamed correctly, then a new replica can be created.

Linked work

No Links to display.

A.12.4 Logging and monitoring. Objective: To record events and generate evidence.

A.12.4.1: Event logging

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:00

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 18:06

What we do

Standard server build includes log shipping configuration. Logs are shipped to a specific server and interrogated through a tool.

Through our controls relating to management of [Supplier relationships \(A.15\)](#) we gain assurance that our logging and monitoring requirements will be met. Suppliers have been selected on a number of criteria for consideration including logging and monitoring capabilities.

For our online Games

All of our applications are built with logging in mind. In order for us to understand their performance they emit information on their performance to the log. The information is written to the system log to the app servers that run our services (which writes to our centralised storage). This allows us to search for interactions with game content or players at a detailed level including requests and responses between systems such as wallet and game.

Information is also stored in the database to offer a transaction and finance based ledger to offer time stamping, quantity of bet and win alongside user records. Our service providers have been selected on the basis of being able to provide appropriate logging, monitoring, alerting and investigation capabilities which are in accordance with legal and regulatory requirements including GDPR and DPA. These are designed to support customer requirements also, including regulator investigatory and reporting requirements.

For our documentation and file storage

We use a cloud service provider in regard to internal documents outside of our ISMS.online instance. The service provision includes logging, monitoring, alerting and investigation capability and compliance with GDPR, DPA and other relevant legislation and regulation.

Linked work

No Links to display.

A.12.4.2: Protection of log information

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:00

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 18:12

What we do

Game and transaction information is written to a central repository.

Only a very small number of individuals have access to production servers - who nonetheless do represent a small risk of internal fraud. However the logs written to central information repository are eadable by all. This offers a level of scrutiny which offers appropriate security, since nobody has access to the logs themselves other than through a read-only tool.

For our online services

Our cloud service providers have been selected on the basis of being able to provide appropriate logging, monitoring, alerting and investigation capabilities which are in accordance with legal and regulatory requirements including GDPR and DPA. These are designed to support customer requirements also.

For our documentation and file storage

We use a cloud service provider in regard to internal documents outside of our own ISMS.online instance. The service provision includes logging, monitoring, alerting and investigation capability and compliance with GDPR, DPA and other relevant legislation and regulation.

Linked work

No Links to display.

A.12.4.3: Administrator and operator logs

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: 21/04/2024

Status: Completed

Approved by Helen Walton on 08/05/2024 09:01

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/03/2022 at 12:13

What we do

Game and transaction information is written to a central repository. Standard server build ships logs to monitoring server.

Only a very small number of individuals have access to production servers - who nonetheless do represent a small risk of internal fraud. However the logs written to central information repository are readable by all. This offers a level of scrutiny which offers appropriate security, since nobody has access to the logs themselves other than through a read-only tool.

An audit log is shipped to the central repository (and stored for 6 months), which is reviewed regularly as part of the ISMS review board.

For our online services

Our cloud service providers have been selected on the basis of being able to provide appropriate logging, monitoring, alerting and investigation capabilities which are in accordance with legal and regulatory requirements including GDPR and DPA. These are designed to support customer requirements also.

For our documentation and file storage

We use a cloud service provider in regard to internal documents outside of our own ISMS.online instance. The service provision includes logging, monitoring, alerting and investigation capability and compliance with GDPR, DPA and other relevant legislation and regulation.

Linked work

No Links to display.

A.12.4.4: Clock synchronisation

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:01

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 17:55

What we do

For our online services and cloud-based document and file storage, time synchronisation is part of the standard provision by the cloud service providers.

Clock synchronisation on workstations and laptop devices is done from an internet accessible atomic clock via NTP. All servers have NTP added and the time source set at the point that they are built

Synchronisation occurs automatically on a regular basis to ensure consistent time is applied across devices.

Linked work

No Links to display.

A.12.5 Control of operational software. Objective: To ensure the integrity of operational systems.

A.12.5.1: Installation of software on operational systems

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:01

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 18:43

What we do

Installation of software carries differing risks depending on the operational system.

In general, however, installation onto operational systems is treated just like any other change - that is, the changes occur within a controlled change management and release process that gives a full audit trail and

logs.

Where dealing with third party systems much of the installation of software is managed by the cloud service providers.

Through our controls relating to management of [Supplier relationships \(A.15\)](#) we gain assurance that installation of software on operational systems is appropriately controlled and managed. Suppliers have been selected on a number of criteria for consideration including operational maintenance.

All changes to operational software are managed in accordance with our policy for [Change management \(A.12.1.2\)](#).

All changes are also carried out according to our principles of:

- Minimal - only packages necessary are added
- Consistent - the same baseline system is used on all three environments: development, staging and production.
- Specific - only those packages which are necessary for the specific function of the specific server or system unit shall be used, without duplication between servers of redundant packages.
- Timely - a regular cadence of releases will see changes and patches applied as necessary. Careful monitoring will alert the team when a hot fix is required which can be released outside of the release cadence but using the release process.
- Auditable - any changes applied either to existing capabilities or to introduce new capabilities to the server are done in code and so a version is maintained as well as an audit trail.

Processes to support the principles

Minimal

G Gaming builds and maintains a known version of a Debian operating system which is used to build each of the three environments: development, staging and production. Changes to that operating system only occur at the point at which an upgrade to the next version becomes available. At this point a full review of the packages available as part of the upgrade takes place and we remove any which are unnecessary for the minimal functioning of the operating system.

Consistent

Because we configure the operating system by removing packages, we know that we can pull the system down from its central store (checking only the minimal set is taken to match our baseline image). The baseline image is used to build all three environments to ensure all three match. This is important from a configuration and maintenance perspective so as to know that changes applied by a developer will behave identically in each environment.

Specific

Each of the roles of the systems are categorised and captured within a server inventory. Only those pieces of software and packages applicable to a given role are installed on a server which fulfils that role. For example, a database server requires differing packages to an app server and the two will not duplicate unnecessary packages of one another.

Timely

All configuration playbooks are run on a weekly basis, irrespective of whether there are queued changes or not. In the event that queued changes exist, the changes will be reviewed prior to the deployment taking place

and the changes will have been deployed to the development and staging environments for a period of time to ensure testing has taken place.

Each week, the available updates to installed packages are reviewed and those deemed fit for upgrade are applied as part of the same automated process.

Announcement channels are monitored for any hot fixes or urgent security updates for packages within the Debian ecosystem. In the event that one needs to be rolled out, the same set of playbooks used on a weekly basis are used to apply the necessary patch. This will still go through the above-mentioned process of release.

Tested

Changes are only ever promoted through the relevant environments. No changes can be made in production without having first been tested in staging and environment.

Auditable

Audit and monitoring take place in two ways: an audit trail for any changes which are made and deployed via automated tooling; in addition, a set of monitoring tools publish logs on what packages are installed and updated on the servers. Change logs are shipped to a central system for broader review and monitoring to ensure changes cannot be made secretly by one or a small number of rogue actors.

For our websites

As for our online services except:

- Rollback process are not deployed as changes are small and easily reversible

Linked work

No Links to display.

A.12.6 Technical vulnerability management. Objective: To prevent exploitation of technical vulnerabilities.

A.12.6.1: Management of technical vulnerabilities

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:02

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 19:12

What we do

G works within an environment within which technical vulnerabilities can have severe consequences for our players, our customers, our regulators and ourselves.

Fraud and malpractice are high risks in the gaming industry, with numerous attacks on a regular basis that intend to exploit gaming software to win money unjustly or steal from other players (in the case of multiplayer games). Such incidents can have heavy financial consequences in and of themselves and can be equally destructive to reputation.

Other vulnerabilities may mean that accidental damage may occur which, while not the result of deliberate exploit, may also have an impact on players and customers. For example, a vulnerability might permit unsafe play by bypassing controls on bet amount or time limits or even exclusions, which can lead to fines, regulatory sanctions and - not least - actual harm to players.

It means that technical vulnerabilities must be taken extremely seriously by G with a focus on handling them at every stage of the process through design, operation, maintenance and improvement of our systems.

Any vulnerability - whether exploited or not - of which we do become aware must be raised and reported using our [Incident Handling Process A.16.1](#).

General

The CTO and Development Teams must keep up to date with news on general vulnerabilities and vulnerabilities that relate to the software services being delivered and other relevant services.

We obtain information on relevant vulnerabilities through [Contact with special interest groups \(A.6.1.4\)](#).

Periodic vulnerability scans and penetration tests are carried out to look for any vulnerabilities not previously identified.

Where a vulnerability comes to light, regardless of the source, it is considered by the CTO along with other key stakeholders as required. The CTO will update the [risk treatment plan](#) for the ISMS accordingly. If the risk requires treatment, then based on the nature, probability and impact of the risk we will decide on one of the following options:

- action is taken immediately;
- schedule for action to be taken by a specified target date;
- the action will be determined as part of the next [Management Review Board meeting per \(9.3\)](#) or via dynamic discussions in that Board working area.

All changes are carried out in accordance with our policy for [Change management \(A.12.1.2\)](#).

Vulnerabilities identified relating to the cloud services we receive from suppliers are managed in accordance with our controls for [Supplier relationships \(A.15\)](#)

Regulatory Scans

Several of the jurisdictions in which we operate require regular penetration tests and vulnerability scans to be carried out on an annual basis (some are more frequent). These audits are carried out by an accredited third party supplier.

An audit of our security policies and processes is also undertaken internally and an audit is required from an external auditor as well - for some regulations this is done in advance of a licence being granted. For others it is an annual event.

Development, Testing and Configuration Processes

An awareness of vulnerabilities (and their potential impact) is baked into product design. This means that each project kick-off requires consideration to be given to potential vulnerabilities. Nested feedback loops, including regular testing of the 'whole' product by people not involved in its development are also part of our testing and release procedures. Peer review, logging and other processes related to release management are also designed to ensure a more secure technical and development environment. Finally, third party testing and certification is required for each game which offers an external check for some vulnerabilities.

To minimise the likelihood of vulnerabilities, careful consideration to system design, infrastructure security and the potential for internal fraud is baked into how we provision and configure our systems as a whole.

Such a process is not exhaustive, of course. Vulnerabilities which the team had not considered are found and their resolution and prevention is dealt with via the Incident Handling Process.

Linked work

No Links to display.

A.12.6.2: Restrictions on software installation

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:02

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 19:15

What we do

Devices

We do not impose any general restrictions on the installation of software on users' local devices as long as they act in accordance with our:

- [Terms and conditions of employment \(A.7.1.2\);](#)
- [Code of conduct;](#) and
- [Acceptable use of assets policy \(A.8.1.3\)](#)

Systems

As part of our controls for [Management of technical vulnerabilities \(A.12.6.1\)](#) as well as our [Control of Operational Software \(A.12.5.1\)](#), there are significant restrictions on the installation of software packages to our operating systems.

Linked work

No Links to display.

A.12.7 Information systems audit considerations. Objective: To minimise the impact of audit activities on operational systems.

A.12.7.1: Information systems audit controls

Assigned to: Dan Rough

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:03

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 19:46

What we do

The implementation guidance for ISO 27002:2013, [\(A.12.7.1\) Information systems audit controls](#) will be applied as appropriate depending on the systems under audit, the assessed risk levels and the nature of the audit.

Audit requirements for access to systems and data will be agreed with appropriate management in the [Management Review Board per \(9.3\)](#).

The scope of technical audit tests will be agreed and controlled with the CTO;

Wherever possible, the following must be applied:

- Audit tests will be limited to read-only access to software and data;
- Access other than read-only will only be allowed for isolated copies of system files, which must be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;
- Requirements for special or additional processing must be identified and agreed;

- Audit tests that could affect system availability will be run outside business hours; and
- All access will be monitored and logged to produce a reference trail.

Linked work

No Links to display.

A.13. Communications Security

A.13.1 Network security management. Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A.13.1.1: Network controls

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:04

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/03/2022 at 11:25

What we do

Our network diagram shows the connections and segregation in our networks and how client data is stored separately on AWS servers.

We primarily use cloud-based services like AWS for our operations.

The cloud-based service providers is responsible for their own network controls including:

- Network authentication;
- Network services availability;
- Network protection controls such as:
 - Authentication mechanisms;
 - Firewalls;

- Anti-denial of service technologies;
 - Anti-malware controls; and
 - Intrusion detection & prevention technologies.
- Segregation and encryption of data flowing within their network(s);
 - [Logging and monitoring \(A.12.4\)](#)

We gain assurance for the provision of these services through our controls relating to management of [Supplier relationships \(A.15\)](#). As the services we take are from large commercial cloud suppliers, the network services agreement forms part of the suppliers' terms and conditions and includes support 24/7

To ensure that our interactions with cloud-based services remain secure, connections use the TLS protocol to create an https session.

Encryption of internet sessions

For connection to our developed online services:

- Uses a 2048 bit RSA key
- Key material is signed using SHA-256 with RSA Encryption

For connection to our cloud-based document and file services:

- Uses elliptic curve cryptography
- Uses a 256 bit key with a 256 bit base point order length
- Key material is signed using SHA-256 with RSA Encryption

Documents



[Bornlucky Infrastructure - Prod Staging Dev Multibox.pdf](#)

Added: 08/03/2022 Added by:

[Helen Walton](#)

Version: 1.0

Linked work

No Links to display.

A.13.1.2: Security of network services

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:05

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 21:23

What we do

G Gaming's hosting providers, currently Amazon Web Services in the UK and Sapphire in Gibraltar, are ISO 27001 compliant. As such, G Gaming's infrastructure meets all requirements from a network control perspective. When a need arises to consume functionality from a provider outside of our own infrastructure (e.g., payments), all suitable measures must be put in place to ensure information remains secure.

Our security controls ensure secure connections between our local devices and the cloud services and this is covered within [Network controls \(A.13.1.1\)](#).

Linked work

No Links to display.

A.13.1.3: Segregation in networks

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:05

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/03/2022 at 11:28

What we do

Segregation in Networks is covered through the separation of our environments: development, staging and production. This is covered in our policy: [A.12.4.1 Separation of development, testing and operational environments](#)

Configuration Management

All changes to the architecture are managed through our [Change management controls \(A.12.1.2\)](#) including firewall rule changes.

Access control rules throughout the network are managed in line with our [Access control policy \(A.9.1.1\)](#).

Linked work

No Links to display.

A.13.2 Information transfer. Objective: To maintain the security of information transferred within an organisation and any external entity.

A.13.2.1: Information transfer policies and procedures

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:06

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 20:13

What we do

We rarely transfer data files between our organisation and customers or suppliers, and it is almost always anonymised - that is, not traceable to any particular player or customer. Nonetheless on occasions where a data transfer might occur, the policy identifies the methods and rules for such transfers.

For more regular communication, other controls within this ISMS apply (e.g. for the use of e-mail).

Policy

This policy describes the preferred methods of transferring data.

Whilst other methods are available, and customers or suppliers may dictate their preferred method, these are the ones that we deem to be the most appropriate for Private or Confidential Data.

Policy Statements

1. Prior to any data being transferred, there must be consideration of the requirement of the project and the data that is required.
2. Only data required for specific business purpose(s) is to be transferred. That is, any data not to be used for the specific project must be removed prior to transfer.
3. We will always use one of our preferred transfer methods unless specifically requested to use another method by a customer or supplier.

4. Customer or supplier requirements for the transfer will generally be complied with unless there is deemed to be a significant risk to us from any requested insecure transfer.
5. Any transfer of personal data must be covered by a transfer agreement either as a separate document or as part of contractual documentation.

Preferred Transfer Methods

1. **SFTP:** The primary recommendation for data transfer is through the use of SFTP. This method allows data to be uploaded to or downloaded from a site, accessing it via a username and password. This method ensures that data is transferred over an encrypted tunnel limiting the risk of a "man in the middle attack". This method allows timely data transfer without the need for physical media and transport.
2. **FTP:** The secondary recommendation is the use of FTP. This is not as strong as SFTP as it doesn't use encryption methods while the data transfer occurs.

Best practice for the above methods is to ensure that the data transferred is compressed within a password encrypted file. This will limit unauthorised access to the file should someone access the site.

Other Transfer Methods (Not Recommended)

- **Email:** It is not recommended to supply data via email. If a client asks us to supply their data via this method, it should be made clear that this is not a secure method and that they must take responsibility for it. If it is supplied by this method, then suitable encryption and Password protection must be in place. Passwords must never be emailed with the file.
- **Internet/Web services:** Information transferred via this method should be carried out using https rather than http. Https will ensure that information is passed over an encrypted connection to safe guard the information being exchanged during transmission.
- **Physical media** - We do not want to use physical media if it can be avoided. Always recommend SFTP over anything else. However sometimes it is unavoidable when dealing with large files. If physical media is used the following rules apply:
 1. Media must be supplied in suitable robust packaging using a delivery method that requires a signature of a named recipient.
 2. This must be a traceable delivery method.
 3. Data held on the media must be in a compressed, encrypted and password protected file.
 4. Hard drives must be installed with encrypted volume software (e.g. True Crypt).
 5. The recipient must be made aware that the package is being sent, its estimated delivery date/time, the information it contains, and the passwords required to access prior to the package being sent.
 6. Any password must be communicated separately and must not be included within the same package.
 7. When returning USB devices to clients, the data must be securely removed from the device first.

Linked work

No Links to display.

A.13.2.2: Agreements on information transfer

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:06

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 20:18

What we do

Formal agreements relating to information security, including the transfer of information, with customers, suppliers and other interested parties is maintained in accordance with our controls for [Supplier \(and other important\) relationships \(A.15\)](#).

Contracts, agreements and other documents are stored in the relevant area of our Dropbox files.

Linked work

No Links to display.

A.13.2.3: Electronic messaging

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:06

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 20:22

What we do

For "Public" information

- Facebook, Twitter, LinkedIn, Blog (for public marketing and customer communications)

- Email (IMAP provided by gmail)

For "Open" Information

- Links to our Dropbox files
- PDF expiring links to Airtable individualised Roadmaps
- Email (IMAP provided by gmail)
- Links to shared googledocs or googlesheets

For "Private" information

- General work content - communications, collaboration via Slack, Notion Github, Skype
- Email (IMAP provided by gmail)

For "Confidential" information

- SFTP transfer preferred, as per [Information transfer policies & procedures \(A.13.2.1\)](#);
- E-mail only if absolutely necessary and:
 - Must only be sent if the information is adequately encrypted; and
 - Only if prior approval from the information owner is in place.

Email security requirements

- Access via webmail must be over HTTPS;
- Access via an email client must use TLS/SSL.

Linked work

No Links to display.

A.13.2.4: Confidentiality or non-disclosure agreements

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:08

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 20:23

What we do

Internal

Internally, rules relating to confidentiality and non-disclosure are covered in our:

- [Terms and conditions of employment \(A.7.1.2\)](#);
- [Code of conduct](#); and
- [Acceptable use of assets policy \(A.8.1.3\)](#)

External

Formal agreements relating to information security, including confidentiality and non-disclosure, with customers, suppliers and other interested parties is maintained in accordance with our controls for [Supplier \(and other important\) relationships \(A.15\)](#).

Each agreement type is considered a starting point (unless it is a non-negotiable agreement e.g. for software licensing).

When in a negotiation and a version of the confidentiality agreement is in use, it gets version controlled in its own right and the history is kept within the relevant customer, supplier or partner account area in our secure platform, or associated to the order history if an online agreement is followed and no explicit signature is required from either party.

Authorised company signatories where a document needs a signature and does not deviate from the standard include:

- Any Director
- CFO

Authorised signatories for agreements that are introduced by other parties or are negotiated variances from our standard are:

- CEO
- CFO
- CCO
- CTO

Documents

 [99Royale Platinum Addendum.docx](#) Added: 08/05/2024 Added by: [Helen Walton](#) Version: 1.0

 [Data Processing Agreement.docx](#) Added: 03/03/2022 Added by: [Helen Walton](#) Version: 1.0

 [Std G Reseller Games Supply.docx](#) Added: 03/03/2022 Added by: [Helen Walton](#) Version: 1.0

 [Mutual-Non-Disclosure-Agreement.docx](#) Added: 03/03/2022 Added by: [Helen Walton](#) Version: 1.0

Linked work

No Links to display.

A.14. System Acquisition, Development and Maintenance

A.14.1 Security requirements of information systems. Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A.14.1.1: Information security requirements analysis and specification

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:08

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 16/04/2024 at 12:50

What we do

The organisation follows the security controls as specified throughout this ISMS which include the assessment and documentation of security requirements, especially:

- [Information security in project management \(A.6.1.5\)](#);
- [System change control procedures \(A.14.2.2\)](#); and
- [Information security policy for supplier relationships \(A.15.1.1\)](#).

For in-house developed applications or software

Information security requirements are considered and documented during the design phase and then throughout the project lifecycle in accordance with [\(A.6.1.5\)](#).

EU GDPR requires privacy by design including privacy impact assessments and that is also incorporated within A.6.1.5 and more broadly described in the GDPR compliance environment.

For “Commercial, off-the-shelf” (COTS) software

Project management controls from [\(A.6.1.5\)](#) are followed.

Assessment of the information security requirements will form part of the consideration for selecting competing packages/solutions. This will include, where necessary, a risk assessment relevant to the use of the software and the information assets within. We review the problem we are trying to solve at the point at which we are reviewing software service vendors to determine what the appropriate security requirements are.

For cloud services

Project management controls are again followed.

As with the procurement of COTS software (above) information security requirements will be assessed, and a risk assessment carried out where a cloud service is being considered.

We use leading services for our information needs. The process for the acceptance of information systems provided by external suppliers is specified in the [Information security policy for supplier relationships \(A.15.1.1\)](#).

Linked work

No Links to display.

A.14.1.2: Securing application services on public networks

Assigned to: Unassigned

Days estimated: 0.0

Days taken: not set

Due: 08/03/2023

Status: Completed

Approved by Helen Walton on 08/05/2024 09:09

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/03/2022 at 12:21

What we do

For our software services

We secure the confidentiality, integrity, authenticity of the communicating client and actions they may perform across the transport and application layers.

Transport layer

Communication with the service must use HTTPS which protects the confidentiality and integrity of the data during transmission.

Where exceptions to this exist as per a Customer's request, a risk assessment will be carried out in advance.

Application Layer

- **Authentication**
 - The user authenticates with a username and password.
 - On successful authentication the application sends the user a token that is used to authenticate the user for subsequent communication in their session.
- **Authorisation**
 - Based on the business rules of the application.

For our websites

The information on the website is completely public. There are no requirements to secure the communication of data to and from the site.

For cloud services

Our use of cloud services is via HTTPS or a similarly secure protocol (e.g. SSH).

Services that don't offer a secure connection must be evaluated to ensure that the security risks are acceptable.

Encryption of internet sessions

For connection to our developed online services:

- Uses a 2048 bit RSA key
- Key material is signed using SHA-256 with RSA Encryption

For connection to our cloud-based document and file services:

- Uses elliptic curve cryptography
- Uses a 256 bit key with a 256 bit base point order length
- Key material is signed using SHA-256 with RSA Encryption

Linked work

No Links to display.

A.14.1.3: Protecting application services transactions

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:12

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/03/2022 at 12:27

What we do

A “transaction” in this control refers to any authorised request made to a web service.

For our developed products and services

The general aspects are covered by our controls relating to [Securing application services on public networks \(A.14.1.2\)](#).

Transaction failure

Failure should not occur, however, given the volume of transactions, many of our systems are designed to fault tolerant. A set process for coping with Failure is written into our integrations with Operators. Thus a retry frequency and time period along with reactions to specific errors, will be created as part of each integration. There are however circumstances in which the level of failures (whether dealt with or not) is regarded as concerning. In these cases, an alert is pre-set to warn developers when a certain number of failures on a particular system are reached to create an incident which will then be managed appropriately.

In all cases (whether retried or not) failure information will be recorded in the system log for further investigation where required.

For our public websites

Covered completely by our controls relating to [Securing application services on public networks \(A.14.1.2\)](#).

For other services

Covered through supplier policy controls in [Information security policy for supplier relationships \(A.15.1.1\)](#)

Linked work

No Links to display.

A.14.2 Security in development and support processes. Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

A.14.2.1: Secure development policy

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:13

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 21:37

What we do

The policy below reflects our approach to secure development of our online services and websites.

Many other controls within this ISMS also provide security in the development process, especially:

- [System change control procedures \(A.14.2.2\)](#);
- [Information security in project management \(A.6.1.5\)](#); and
- [Information security requirements analysis and specification \(A.14.1.1\)](#).

Policy

Policy Statements

For our software

1. All developments will be:
 - a. carried out by competent, authorised individuals;
 - b. carried out in a secured development environment;
 - c. be subject to thorough testing, including negative testing, load testing and impact testing as appropriate to the level of change through automated and manual testing;
 - d. be subject to thorough quality assurance/peer review prior to implementation; and
 - e. only put into production once all testing and authorisation has been completed.
2. Consideration for security requirements will be included in the design phase and be followed through the development lifecycle as per [\(A.6.1.5\)](#) and [\(A.14.1.1\)](#);
3. Code will be stored in secure storage libraries;
4. Version control will be maintained throughout;
5. System documentation is to be maintained which includes information about security elements. Such documentation will be classified as "Sensitive";
6. Consideration for the use of secure coding standards will be given for each project; and
7. Where outsourced development is considered, such external developers will be made subject to the same conditions as internal developers.
8. Outsourced developers will be selected in accordance with our [Information security policy for supplier relationships \(A.15.1.1\)](#)

Procedures to support the principles:

Developers run a mirror of the production environment on their local machine so as to replicate the full software stack as closely as possible. Automated tests are triggered after each significant commit to check whether the changes introduced have affected other parts of the software. Together, these processes provide real-time testing of every change, meaning that fewer errors are made in the early stages of development. It also provides early insight into any necessary changes software-wise in the existing production environment, such as any new dependencies, allowing further testing and exploration where necessary.

Development work is undertaken on a branch-per-feature basis. No developer is permitted to publish his or her own software changes to the master branch. Instead a merge request is issued including documentation around the change, its risk and its expected behaviour. A second developer accepts receipt and begins a check. When the check has passed successfully, he merges the changes into the master branch. This triggers a second notification informing the original developer.

This means that a developer other than the one who authored the code will perform checks on the code's security, fault tolerance, performance and logging, as well as a coding standards review, before it makes its way into the main branch. There are two main benefits of this approach: it ensures that break fixes can quickly be shipped to a production environment, and that any changes not yet ready to commit are segregated so that they can be developed and tested in isolation.

This is best practice which allows us to have high confidence in changes to the actual production environment, offering further quality assurance to users and customers. A further quality control feedback loop is also present since changes to the hosting infrastructure will then be subject to the Release And Change Control Process.

Consequences of non-compliance with this policy

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.14.2.2: System change control procedures

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:14

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 09:14

What we do

The Release and Change Control processes which Gamevy employs are the last point in a rigorous series of processes which aim at a zero defect rate and are part of our overall quality assurance program. G subscribes wholeheartedly to the philosophy of continuous testing, of nested feedback loops and of automated layers of development, integration and deployment tests interwoven with manual checks. We do not accept any trade-off between speed of release and reliability of service, since our layers of process are kept light-weight, but rigorous through automation.

It builds upon the principles and controls set out in [\(A.12.1.2\) change management](#).

What is a change?

A change is considered to be the alteration of any product that has the potential to impact a customer either from an Operations or Software perspective (as opposed to Business process changes which are dealt with through the individual operational functions such as marketing, finance etc).

The term 'change' can range from tiny performance tweaks up to the launch of new games. We differentiate between changes in terms of impact and risk to the customer. For our purposes, hardware and software changes are treated alike.

Before a software change is made, the change needs to be assessed for whether it will have a significant impact on the outcome of a game for a customer. If a change will change any of the critical hashes as documented within the game's UK GC certificate then the change must be classified as major and will trigger a re-certification process. See the scoring implemented in [\(A.12.1.2\) change management](#) for examples of other levels of change 'risk' and how they are managed before a change can be passed as having potential for release.

Revision History

As new features and products are developed, the configuration attributes are defined within the application code. The attributes are described using our current automation framework, Ansible. Following this practice means that the attributes which make up a Configuration Item are baselined from the outset. As each change is stated explicitly in code, a revision history is available owing to the fact that the code is stored in Version Control.

Development and Testing Controls

The series of automated tests and principles of code review are described in [System acceptance testing \(A.14.2.9\)](#). This means that even small changes are fully reviewed before being merged into the codebase following a set of automated tests and a process of manual review that includes a risk assessment of the change and a documented way to test the change. The comments and input of both the proposer and the reviewer are recorded and both are deemed responsible for the change.

Candidate for Release

Following a change having been merged and having been passed as potential for release (that is not triggering sign off from a customer, third party or certification through our rollout process), it becomes a candidate for release into production. This requires a further set of tests using production configuration, a review and risk assessment using the procedure described below.

Release

The core aspects of G's releases are automated and take place seamlessly in the background.

Automation means that the possibility of human error is reduced, while by releasing frequently, and consequently keeping the changesets small, the risk involved in each release is reduced. The benefits are:

- Zero downtime deployments - customers do not experience interruption.
- Ease of roll-back - any change deployed to production can be rolled back to a previous state, instantly switching away from any error, also without interruption.
- Constant performance - automated monitoring of the system means any issues are flagged instantly and the system can be rolled back to the previous working version, allowing us to investigate any problem.

Although all releases are automated in terms of the mechanics of how they occur, the release to a production environment is triggered by a qualified and competent individual taking an action within our build management system, Jenkins.

Low Risk - where the release risk has been quantified as Low and does not trigger any requirements for regulatory sign-off, it can be performed following G's standard continuous deployment methods. That means it can occur at any time and can be unattended - it relies on a comprehensive suites of automated tests rather than any human intervention. An example might include a change in the default bet for a particular customer following a request, or a correction to a typo in a set of rules.

Medium Risk - where releases are deemed to be of Medium risk, the release must occur during business hours so that they can be live-monitored by the people implementing the change. An example might be the launch of a game (which has separately been fully certified ready for release via our rollout process) or a new integration going live.

High Risk - for a release that contains a high degree of risk, the team set aside an agreed Maintenance Window during which the release will be made. This will be planned in advance for a particular time. Customers are informed of the Maintenance Window, and no play is allowed during that time. This permits G to monitor a release in absolute safety in a live environment before introducing real customers. An example might be a new database switch over.

Monitoring

Monitoring of the production system ensures that after a release has taken place, any problems that occur can be identified before they affect customers. A set of key metrics are monitored and compared against known baselines to identify any trends suggestive of problems. At pre-arranged trigger points a notification is sent to the developers involved who investigate and take action accordingly. For medium risk releases, developers are expected to be monitoring the system in person.

Linked work

No Links to display.

A.14.2.3: Technical review of applications after operating platform changes

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:15

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 22:26

What we do

For the devices used by employees and associates

Risk analysis shows that the risk of operating platforms upgrades is tolerated, and no further controls are needed. Staff are made aware of keeping their device operating systems up to date.

For software we produce

Operating platform changes are first tested on a staging server that is separate from the production environment. The staging server is a mirror of the production server, with the exception that its resources for dealing with load may be many times less than a single production server.

We satisfy ourselves that the change is acceptable by:

- Performing the system testing set out in [System acceptance testing \(A.14.2.9\)](#);
- Re-running all of the lower level integration and unit tests on the staging server;
- Inspection of the performance characteristics of the staging server resulting from system testing in accordance with our controls relating to [Capacity management \(A.12.1.3\)](#).

If any of these steps show that the upgrade impacts the functioning of the system, then we take the following action:

1. Determine the scope of the impact;
2. Determine whether the value in postponing / not performing the upgrade vs the potential time to research causes and fixes for the impact are worth investigating;
3. If we choose to research the causes of the impact then:
4. Determine the cause of the problem(s);
5. Examine fixes for the problem(s);
6. Determine whether fixing is viable vs postponing / not performing the upgrade;
7. If fixing is viable then apply fixes and repeat this upgrade process from scratch;

The CTO or Senior Developer is responsible for the overall co-ordination of this process.

If the operating platform change affects our business continuity plans, then they will be updated accordingly.

For our websites

Operating platform changes are applied under our own volition. When a change is made, we perform a manual inspection of the website to ensure that the change has no negative impact.

The nature and extent of any change will determine the amount of manual inspection that is required.

For other services

Our other services are supplied by cloud service providers and such changes are covered under our controls for [Supplier relationships \(A.15\)](#).

Linked work

No Links to display.

A.14.2.4: Restrictions on changes to software packages

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:15

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 22:28

What we do

For technical employees

Technical employees may modify the software on the devices they use for work. This is only permissible if the licence of the software permits it (e.g. most open source software is licenced under terms which permit it to be modified). However, as modifying software takes effort and introduces risk it should only be considered where there is business value to be gained. For example, fixing a bug that is hampering development if the maintainer of the software is unwilling to fix the bug themselves.

For organisation-produced software and public websites we use

In this case modification is taken to mean one of the following:

- modification to software that is external to the application code that comprises our software (e.g. customisations to the database service)
- modifications to the software libraries that are used directly by the application code (e.g. libraries that integrate the search service into the application itself)

We do not make changes to software unless there is a strong business case to do so.

We only modify software whose licence terms are compatible with those of our software.

Where changes are necessary, we consider the following:

- Where the changes to the software are likely to never be incorporated into the software then we consider extracting our changes into a discrete layer that overlays the core software. This simplifies the process of updating the software whilst retaining our changes.
- If the change is likely to be incorporated into the software, then we make the change to a 'branch' of the software and issue a request to the software maintainer to merge in our changes. Once the changes are merged in then we switch to use the official release of the software.

Both of these approaches give us an easy way to identify the divergence from the original software.

In certain cases where the change is particularly invasive, we may choose to make the changes directly to the software. Generally, we only do this when the software is reaching the end of active development or we are certain that we won't be needing to rely on future updates.

Modifications to software are subject to the systems acceptance testing process defined in [\(A.14.2.9\)](#).

Linked work

No Links to display.

A.14.2.5: Secure system engineering principles

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:15

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 22:33

What we do

For our developed platforms

General approach:

- Security is everyone's responsibility.

- Security issues often present themselves at several points in the development lifecycle and these are addressed as part of our agile production process.
- Peer review takes place to help identify any security concerns or opportunities for improvement at various stages, including team estimating, planning, code review and independent testing.
- Changes to architecture that has security implications is subject to more stringent checks in all stages of the development lifecycle.
- We keep up to date with best practice and news relating to relevant job roles and system engineering principles including [Contact with special interest groups \(A.6.1.4\)](#).
- We favour close collaboration and talking rather than detailed written exchanges.
- We document dynamically - that is our tests, acceptance tests and merge requests form the documentation for much of our code.

Technical principles:

- We design and implement architectures that standardise how security features are handled (e.g. the framework that our software runs on provides many security features out of the box)
- Technical solutions are as simple and as minimal as possible to reduce legacy 'noise'
- Automated tests exist for all code.
- Security issues are addressed at the root level.
- We continue to investigate tools that can automatically detect vulnerabilities (static code analysis, penetration testing tools, etc.)
- Security architecture is designed and reviewed by senior engineers.
- We apply the principles of defensive coding wherever possible.

When a security vulnerability is discovered:

- A full analysis is performed to discover the extent of the vulnerability.
- We investigate how we can avoid similar vulnerabilities occurring in the future.
- Where appropriate based on the time / lifecycle development position of finding the vulnerability, improvements are captured in the [ISMS Corrective Actions & Improvement Track](#).

Our [Secure development policy \(A.14.2.1\)](#) provides more details on how we apply some of these principles.

EU GDPR requires privacy by design including privacy impact assessments which is incorporated within [Information security in project management \(A.6.1.5\)](#) and is more broadly described in the GDPR compliance environment.

Linked work

No Links to display.

A.14.2.6: Secure development environment

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:17

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 21:54

What we do

For organisation produced software

The development environment is completely isolated from the production environment as per our controls relating to [Separation of development, testing and operational environments \(A.12.1.4\)](#).

Development is performed on the local device of the developer be they internal or external.

The following apply:

- Production data is not allowed to be stored on the local devices of developers;
- Access to the codebase is controlled under our [Access control policy \(A.9.1.1\)](#);
- Changes to the codebase are controlled under [System change control procedures \(A.14.2.2\)](#).
- Our codebase is held securely in private repositories at GitHub.com (a cloud based Distributed Version Control System (DVCS)).
- Where development is outsourced see [Outsourced development \(A.14.2.7\)](#).

Changes to the development environment

There are three levels of dependencies in the development:

1. The version of the language used to run the application.
2. Libraries used by the runtime language of the application.
3. Applications and services that the application interacts with (e.g. database).

1) This is managed by each developer. A change to the runtime language version would in most cases be considered a change to the operating platform and would fall under [\(A.12.4.3\)](#). We recommend the use of special version manager software to simplify this task. The application is configured to automatically use the correct version of the language for most popular version managers.

2) We use dependency management software which ensures that each user has exactly the same libraries. This software also ensures that the same libraries are used in the production environment.

3) Application level external dependencies are not strictly managed as there is a very low probability that they introduce incompatibilities. All automated tests are carried out on a build server which uses a known and good

set of external dependencies.

For our public websites

We do not have a standard development environment for the website.

Depending on the nature of development work undertaken we may choose to:

- Perform the work on the live platform (e.g. for trivial template changes).
- Perform the work on a staging environment on the website server itself (e.g. for more substantial template changes).
- Work locally and then synchronise with the staging environment for testing (e.g. for substantial changes covering many parts of the site).

Linked work

No Links to display.

A.14.2.7: Outsourced development

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:17

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 21:51

What we do

General

The selection and use of outsourced software developers is managed in accordance with controls for [Supplier relationships \(A.15\)](#).

Intellectual property rights are set out in formal agreements and are signed by all external software development parties.

All developers are assessed to ensure they are qualified and competent.

Where possible, existing trusted associates are used first, or if not suitable then their network of contacts as a means of recommendation/referral.

EU GDPR requires privacy by design including privacy impact assessments and that is incorporated within Information security in project management (A.6.1.5) and more broadly described in the GDPR compliance environment. Where necessary a Data Processing Agreement will be signed.

For our software

The same controls apply for outsourced development as internal development:

- (A.14.2.1): Secure development policy
- (A.14.2.9): System acceptance testing

For any public websites

The control in (A.14.2.2) for website development applies. For significant work (e.g. new websites) the work may be subject to delivery through controlled project or group for effectiveness and efficiency with the chosen designers & developer/s.

Linked work

No Links to display.

A.14.2.8: System security testing

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:17

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 21:49

What we do

System security testing is incorporated into System acceptance testing (A.14.2.9).

Linked work

No Links to display.

A.14.2.9: System acceptance testing

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:18

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 21:48

What we do

System acceptance and security testing is part of:

- [Information security in project management \(A.6.1.5\)](#);
- [Change management \(A.12.1.2\)](#); and
- [System change control procedures \(A.14.2.2\)](#).

Testing is carried out on all changes to ensure the security, robustness, correctness and performance of the application. It therefore also incorporates Security testing ([A.14.2.8](#)) in this control as well.

Automated Testing

We have a comprehensive and fully automated test suite that verifies the correctness of the application at these levels:

- **Unit testing:** Unit testing is the most granular of our testing suites. They ensure that the individual functions written by a developer behave as expected. This is an automated, comprehensive suite of unit tests verifies the behaviour of components, exercising them with the appropriate boundary conditions. Stubbing and mocking is used to isolate the elements under test and eliminate extraneous setup states.
- **Integration testing:** Integration tests ensure that component code which relies on other functions performs as expected. Normally, but not always, this means that as each new piece of code is added to the whole, an integration test ensures that there are no breaks as changes are introduced. Any break that does occur can be identified, isolated and fixed immediately. Integration testing happens both at a granular level and at a higher level when integrating services, such as those third parties that G is dependent upon - wallet and Geo-Location verification, for example.
- **End-to-End system testing:** these run at the macro level mimicking actions that a customer will make to ensure that the entire back-end system responds using the correct levels of security and reporting. This enables us to be sure that we can trace bets placed and actions taken with absolute confidence. The

actions that would be taken within the client side application are mocked at the moment, since it is difficult to automate tests within - for example - an iOS environment. The end-to-end tests mimic the behaviours that the client side application would be sending to the endpoints.

- Client-side testing: we have created a bespoke suite of client-side tests. These test core functionality, especially of appearance of gaming controls or particular views, while also striving to test performance of the games.
- Security testing: boundary condition, exception testing, and negative impact testing. Optionally for major changes, vulnerability and penetration testing.
- Production testing and monitoring: Following a production release, a set of smoke tests are run which ensure that all core functionality remains intact. In addition, a set of defined metrics are monitored after release.

Manual Testing

Changes are made by individual developers in isolation. For these to be merged with the master branch, a code review must take place.

The code review is done by another developer who has the appropriate skillset to evaluate and test the code submitted.

The review includes as standard:

- that the code meets internal coding standards (style guides, default frameworks, etc)
- that the code contains only functionality that is relevant to the requirement being developed
- that the code's performance will not affect the customer's experience
- that the code has taken steps to meet security considerations
- that there is adequate logging within
- that fault tolerance has been addressed
- that an appropriate amount of tests have been introduced to ensure the functionality in the future and document the requirements

The code review is triggered by a pull request. A pull request must contain detail about the reason a change is being made. Other information, such as who made the changes, the files and lines of code that are affected, and a report on the outcome of the suite of automated tests that ran when the merge request was issued, is provided by the source control system. This information combines to describe a Changeset.

The developer who carried out the code review now has responsibility for merging the code. This means that both developers share responsibility for the change

Regulatory Testing

All games, as well as the RNG and RGS (Remote Gaming System) must be tested by an accredited third party against key jurisdictional requirements before a certificate can be issued which permits the game to be released onto Production for customers.

For other services

Our overarching theme of system acceptance for externally supplied services is that we aim to select leading and well-trusted services that are known for their robustness, reliability and security in accordance with our controls for [Supplier relationships \(A.15\)](#).

Documents



[Testing Flow.png](#) Added: 03/03/2022 Added by: [Helen Walton](#) Version: 1.0

Linked work

No Links to display.

A.14.3 Test data. Objective: To ensure the protection of data used for testing.

A.14.3.1: Protection of test data

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:19

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 03/03/2022 at 22:38

Policy

For organisation produced software

No personal data is used for testing in ordinary circumstances. Moreover even if any operational data were to be used, it is already anonymised, with no connection to an actual identifiable player. Personal data is held by the operator and is not passed to G.

All tests use specific test fixtures that are relevant to the test in question. These fixtures are loaded onto a 'fresh' database which contains no real user records. The access control procedures, which apply to operational application systems, also apply to test application systems;

For our public websites

Business emails may be collected on the website with all appropriate permissions for the purposes of marketing, but there is no need to test with personal data.

Linked work

No Links to display.

A.15. Supplier (and other important) Relationships

A.15.1 Information security in supplier and other important relationships.

Objective: To ensure protection of the organisation's assets that is accessible by suppliers (and other important relationships affecting delivery).

A.15.1.1: Information security policy for supplier (and other important) relationships

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:19

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 16/04/2024 at 12:54

What we do

Considerations in approach to supplier selection and management:

- We have supplier relationships that vary in terms of value and importance, size and scale, where a one-size policy does not fit all.
 - For small suppliers or independent freelancers, unrealistic expectations could drive up cost or damage key relationships by placing unreasonable expectations on them.
 - Our supply chain also includes large commercial suppliers where our ability to influence or control their practices is negligible.
- However, we hold information and records of agreements and strategic activity such as contracts, security requirements, contacts, commercial information (e.g. IPR, confidentiality, financial) in our Dropbox and also in our CRM and finance system.

Our policy for addressing information security with suppliers is attached as a document given its comprehensive nature and it is based on a segmentation approach where we treat the supplier based on its value and importance to the organisation objectives and its risks affecting our ISMS.

Confidential

What are typical information security requirements?

Where an activity is defined as high risk because it relates to highly sensitive data (this may include employee data when applying for a licence, for example, or player transaction data), as a minimum we will require ISO27001 or the North American equivalent SOC2.

Our example agreements covering confidentiality, IP, Data Processing and other key areas are attached in [A.13.2.4 Confidentiality or non disclosure agreements](#)

Policy

See attached policy document.

Documents

-  [Due diligence form.docx](#) Added: 04/03/2022 Added by: [Helen Walton](#) Version: 1.0
-  [Outsourcing & Supplier Policy.docx](#) Added: 03/03/2022 Added by: [Helen Walton](#) Version: 1.0

Linked work

No Links to display.

A.15.1.2: Addressing security within supplier (and other important relationship) agreements

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:20

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 23:20

What we do

As detailed in [\(A.15.1.1\)](#) the organisation has different types of supplier relationship and our approach towards information security varies for each type given the nature of the information and assets being accessed. A contracting lifecycle and in-life segmentation-based approach is also outlined in the policy to help distinguish contracts based on Importance & Risk, alongside Financial Value.

General approach to supplier agreements

ISO 27002 guidance for (A.15.1.2) a - p is considered within supplier agreements, however the organisation recognises that it neither has the financial or physical resources or power to dictate those conditions to all suppliers and it is not necessary for many of them.

A risk-based approach is taken in consideration of the Supplier Type, the contract Risk & Importance along with the Financial Spend to arrive at the appropriate risk-based agreement for the organisation.

We work with suppliers that already meet the majority of our Information Security needs for the services that they provide to us and have a good track record of addressing information security concerns responsibly.

We select leading and well-trusted services that are known for their robustness, reliability and security and wherever possible look to suppliers that have already achieved ISO 27001 or its equivalent.

These points allow us to minimise the amount of information security specific detail in supplier agreements especially where our buying influence may be small.

For providers of technology solutions, regardless of category below, we aim to select service providers that adopt a similar approach to information security in their provision of technology services as we do. This approach is expressed in the controls throughout this ISMS.

The CTO, Management Review Board, or nominated representative will make decisions on risk acceptance for where a provider does not meet those high levels of security or is unable/unwilling to demonstrate it to us (e.g. because we are small), but we still wish to adopt their service.

For Infrastructure Critical suppliers:

- Outsourced, freelance and independent developers agree to the procedures set out in (A.13.2.4) and they are introduced to our ISMS and other relevant working practices they need to adopt, regardless of whether they have their own too. Only once the CTO or nominated representative is happy with compliance does the supplier get access to "Confidential" or "Private" information assets. The supplier's details and contract are held in the relevant [supplier account](#) and they comply with our controls relating to [Outsourced development](#) (A.14.2.7).
- For datacentre hosting providers and other suppliers of this type, the organisation has limited negotiation leverage so is unable to mandate certain practices e.g. right to audit or the supplier's screening processes. However, we only work with these very large suppliers if they hold ISO 27001 or its equivalent in the areas that are important for us.
- Business continuity and assurances for continuing service delivery in the event of a supplier failure or disaster are addressed in the relevant ISMS controls areas.

For Strategic Business Services suppliers:

- These suppliers are very similar to the category above in that they include very large suppliers like banks, and again we have limited influence or control, other than standard banking terms and small business relationship managers. The [supplier account](#) sets out the key contacts and the FD holds other "Confidential" or "Sensitive" information in relevant banking and finance systems as per controls set out in the ISMS. Small strategic business services suppliers like accountant services are governed by specific agreements which address information security and the accountant's codes of practice. We set out to have pragmatic agreements with these small suppliers, managed intimately by the FD and/or CEO. The likelihood of information security risk is assessed to be very low. Where necessary the FD and CEO work together in private communication groups in ISMS.online in regard to the delivery of services by these suppliers.
- All suppliers of this type processing personal data are to have the Supplier's Data Protection Officer details in the relevant account contact area.

For customers and partners:

- We require that they follow agreements and practices outlined in [\(A.13.2.4\)](#) and [\(A.15.1.1\)](#).

Linked work

No Links to display.

A.15.1.3: Information and communication technology supply chain

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:20

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 04/03/2022 at 23:21

What we do

ISO 27002 guidance for [\(A.15.1.3\)](#) a) - i) is considered within the information and communication supply chain however the organisation recognises that it neither has the financial or physical resources or power to dictate those conditions to all suppliers and it is not necessary for many of them. A risk-based approach is taken in consideration of the Supplier Type, the contract Risk & Importance along with the Financial Spend to arrive at the appropriate risk based agreement for the organisation.

As outlined in [\(A.15.1.1\)](#) as well as [\(A.15.1.2\)](#) it also makes clear that the organisation exerts influence and controls in accordance with the information assets at risk, whilst recognising that as a small supplier working with sometimes very large providers (e.g. Datacentre and hosting services, banks etc) its ability to mandate practices down the supply chain is limited. Suppliers are selected based on their ability to meet our needs, for example in accordance with [System Acquisition, Development and Maintenance \(A.14\)](#).

Information and communication supply chain risks are captured in the [risk tool](#) in line within [6.1](#) and treated, then tolerated where appropriate as follows:

- Large providers of Infrastructure Critical services need to be ISO 27001:2013 certified themselves for the areas we contract them for, which offers us appropriate assurances. The certificate, scope statement and statement of applicability will be assessed to ensure the certificate covers our requirements. We also expect they will be better placed to demonstrate even greater depth and control over their supply chain using principles of ISO 27001: 2013.
- Outsourced and specialist freelance developers who access our information and assets are the last main line of supply chain delivery themselves. We address their use of information processing facilities and other security controls by their compliance with this ISMS as expressed through [\(A.13.2.4\)](#) confidentiality

agreements, and developer induction projects where they commit to follow our relevant policies and controls.

- We tolerate the residual risk per (6.1) from Strategic Business Services large providers like banks, and with our small providers like accountants and lawyers as they deliver our service with their in-house resources in accordance with (A.13.2.4).
- Other large Technology and Other Business Services Suppliers who have access to commercial in confidence information are treated in accordance with Annex A 14 as part of the selection process.

Linked work

No Links to display.

A.15.2 Supplier and other important relationship service delivery management.
Objective: To maintain an agreed level of information security and service delivery in line with supplier (and other important delivery relationship) agreements.

A.15.2.1: Monitoring and review of supplier services (and other important delivery relationships)

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:21

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 10:15

What we do

The organisation monitors and reviews supplier services (and other important relationships) based on the relationship value and importance determined with relationship 'tiers', more fully described in A.15.1.1. This also aligns with A.7.1.2 employment terms and conditions as well as code of conduct in so far as commitments and promises can be made by employees during the course of their engagement or relationship activity with suppliers.

Infrastructure Critical Suppliers

- **Outsourced developers and associates** are managed weekly through a demo and/or project 'flow' meeting. Where projects are critical or encountering issues a Daily stand up may also be initiated. This is

Confidential

a recognised technique for 'agile' development.

Problems and issues are to be first addressed at the team level and through the usual bug/issue management tools, then escalated into individual reviews if required which may be documented in the supplier's account area if evidence is required later. This ISMS process is followed for any security incidents and there are no other suppliers in their delivery chain that need consideration.

- **Datacentre and hosting suppliers** - These suppliers are managed operationally on a day to day basis through discussions in the DevOps standup. Monitoring is done by the supplier for its delivery of services as part of its overall operation and the organisation monitors service delivery affecting our hosted services by the controls outlined in [A.12.1.3](#) and the business objectives KPIs, where relevant e.g. on service uptime.

Commercial reviews are undertaken as required. Where necessary, results and actions are to be documented in the account and any tasks delivered within the agreed timescales as evidenced in the account too.

Any operational and service-based changes are addressed using the relevant channels for change requests and documented accordingly e.g. via online portal or secure email into the service desk.

The organisation does not expect contractual rights to audit these suppliers or dictate its supply chain however to retain our business each provider must maintain an up to date ISO 27001 2013 certification (or equivalent) and where appropriate hold related certifications to satisfy Gambling Regulatory requirements.

Security incident management and other processes follow supplier's normal internal ISMS.

- These suppliers should make available documented certification information as required to offer assurance for our organisation and its customers. This does not need to be held on record by our organisation but should be available on request.

Other suppliers

- We have a light touch approach to supplier management of all other services. We manage these suppliers by exception around problems and undertake reviews on need as part of regular organisational growth and change activity.

Contracts and commitments are generally limited time agreements (technology) or fees for services (accountants, promotional gifts, hotels etc). Where contracts are renewed, especially with cloud technology service providers, checks should also be made to ensure their services continue to maintain ISO 27001 or a suitable equivalent. If not then a risk assessment needs to be made by the CTO or CFO and if appropriate new supplier selection processes take place per [A.15.1.1](#).

Changes to supplier services beyond that detailed above for day to day services is addressed within [A.15.2.2](#).

Other important relationships

- Customer relationships are managed in a variety of ways and places, but contracts and key information will be saved on Dropbox and in our CRM systems on airtable. Services are provided in accordance with [A.13.2.4](#) and any contract specific work packages or processes which are agreed and documented within the account.
- Partner relationships are managed in a variety of ways and places, but contracts and key information will be saved on Dropbox and in our CRM systems on airtable. Services are provided in accordance with [A.13.2.4](#) and any specific work packages or processes which are agreed and documented within the account.

- Regulators are not strictly customers or suppliers or partners, but we often need to communicate regularly with them and provide information. Details are held in Compliance folders on Dropbox and the relationships are managed by the CFO, CEO and Compliance Officer.

Linked work

No Links to display.

A.15.2.2: Managing changes to supplier (and other important delivery relationships) services

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:23

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 10:23

What we do

This control aligns with [\(A.15.1.1\)](#) and [\(A.15.1.2\)](#).

Changes to suppliers' services take into account:

- The nature of the change;
- The supplier type affected and the criticality of business information, systems and processes and re-assessment of risks;
- The intimacy of relationship; and
- Our ability to influence or control change in the supplier

For Infrastructure Critical suppliers

- **Outsourced developers and associates** operational changes to work scope are made during the development process as per [\(A.12.1.2\)](#). Changes in other commercial terms or contract details are to be captured in the relevant documentation (held in Dropbox or on the CRM system). Because these suppliers follow this ISMS any changes to that are also addressed with the suppliers in a similar fashion to our own staff.
- **Datacentre and hosting provider** normal operational changes are to be documented in accordance with [\(A.15.1.2\)](#). and material changes affecting the provision of service to the organisation are subject to negotiation as per contract schedules on changes (where available). Any material changes are documented in the supplier account and if additional contractual signatures are required then these

should be uploaded into the relevant contract area as well.

Any material changes initiated by the organisation that affect suppliers are to be discussed with relevant Management Review Board members and decisions taken in accordance with management reviews 9.3. Where change projects are required e.g. for datacentre provider movement they are delivered in accordance with (A.6.1.5).

For other suppliers

- For technology providers processing commercial in confidence information the CTO or their nominated representative will consider the impact of changes as part of their normal operational meetings. Any changes that have a material impact or risk on Infrastructure Critical services will be discussed at the Management Review Board, otherwise agreed locally with the involvement of relevant stakeholders if commercial terms are impacted.
- Where a provider of Strategic Business Services makes changes then the organisation will consider the impact and negotiate with the supplier as necessary, capturing results of the decisions in the private group or the specific communication channel used with the provider.
- Changes for other suppliers are unlikely to have any material impact on the business due to the nature of the services being provided and we tolerate the risk, reviewing changes by exception either by local management, or Management Review Board if it has a wider impact.

For other important relationships

- Changes to customer or partner services are negotiated and documented in accordance with (A.13.2.4) and held within the relevant documentation - either contracts and addenda saved in Dropbox, or additional notes and promotional activity tracked and communicated to Finance.
- Changes to Regulator services will normally require some form of additional certification, sign off or formal submission. These are documented in Notion and new certificates or applications are stored in Dropbox.

Linked work

No Links to display.

A.16. Information Security Incident Management

A.16.1 Management of security incidents and improvements. Objective: To ensure a consistent and effective approach to the management of information

security incidents, including communication on security events and weaknesses.

A.16.1.1: Responsibilities and procedures

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:24

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2023 at 08:53

What we do

An Incident refers to an event which directly affects G Gaming's ability to deliver a service to its customers. As part of G Gaming's commitment to its customers, and to continuous improvement this document is reviewed annually. The Incident Handling process itself also incorporates a process of review and improvements which are fed back into this document for future use.

The procedures for incident response planning are defined in advance of an incident occurring and have been agreed by the Management Review Board.

The CTO takes overall responsibility for setting the Incident Handling Policy.

Principles

G Gaming's Incident Handling process is based on the Observe Orient Decide Act (OODA) loop. Its primary focus is to resolve the problem as quickly as possible without causing customers any loss.

Feedback is vital and so in the case that a solution is not clear, it is suggested that multiple small incursions are made in order to gain feedback that can provide further insight into the root cause.

The Incident Handling Process has two further focuses. It also acts to ensure that all involved and affected parties are continually informed of the status. Importantly a review process is also included. This ensures that any improvements can be discovered and incorporated into future incident handling to further minimise customer impact.

Incident Classifications

All incidents are treated with the same level of discipline. However, in order to ensure that the correct level of attention is given to the communication of the impact of an incident, it is necessary to understand how to classify it.

When an error is discovered, either through auditing of logs, or G Gaming's continuous testing, the error is classified as a Known Error. A Known Error is investigated. The investigation should ask two simple questions: what is the impact of this error, and what is the severity of this error.

When a Known Error is understood to have the potential to affect players, or G Gaming has received an error report from one of its customers, the error is reclassified as a Problem. When something is classified as a Problem, its existence is advertised within G Gaming, and the relevant affected parties are informed.

When multiple cases of a problem are identified, the Problem is reclassified as an Incident. If the impact of an Incident is large, or the problem is severe, the Incident is upgraded to a Major Incident. Both an Incident and a Major Incident are handled using the process defined within this process.

Reporting

Any Incident which triggers the Handling Process will also generate a report. These may be informal or formal.

Informal Reports - these are notes intended for internal consumption only. They will be jointly written as part of the Incident Review meeting, reviewed by the team involved in the meeting, and will be held on Notion (the company's internal wiki) or on the ISMS Incident Management Board. Where relevant notes may be shared with customers via email from our support service.

Formal Reports - these are full written reports which follow a certain structured template and are intended to be shared externally with Regulators, Operators or other stakeholders. All Incident Reports are kept within G's Dropbox system.

Where a Major Incident is an event that must be reported to a Regulator, the submission will be carried out by G's Compliance Officer or Chief Financial Officer. A record of all such reports will also be held as required for Audit.

Note that our SLAs with particular operators have some specific requirements. For example, communication with operators served by an aggregator normally require that a relevant contact from the aggregator is also copied in (Pollard and Relax)

Roles and Responsibilities

When an incident has been identified a group of people who can assist in solving the problem will be brought together as a team.

Someone will be appointed the Incident Leader. The Incident Leader's responsibilities are as follows:

- To follow the Incident Handling Process to bring a conclusion to the incident
- To lead the activities necessary to reach a resolution to the problem
- To involve the appropriate people in delivering a resolution to the problem
- To ensure that adequate information about the problem is being communicated to all affected parties
- To ensure that a review process is carried out and that any actions that come from it are implemented and fed back into the Incident Handling Process

Orient

This part of the problem-solving cycle is about gathering information. Collect current information from as many sources as practically possible. Establish whether the problem is localised, or if it threatens other aspects of G Gaming's operations.

Observe

Analyse the information that has been gathered, and use it to update your current understanding. It is important to establish the extent of the associated impact of a problem. Knowing this will aid with the process of communication.

It is important to continually validate the scope of the incident. Though a Problem has just arisen, it may be the case that the Known Error which caused the Problem has existed for some time. An explicit check should be made to ensure whether the Problem which led to the Incident has had any historical impact.

If new knowledge has been discovered that has increased understanding of the problem, consider communicating this fact further either internally, or externally.

Decide

Assemble the group and canvas opinion. Decide the next set of actions, and when the group will next meet to discuss progress.

Act

Act upon the agreed actions. Ensure that actions are being communicated.

Communication

Appropriate measures should be taken to communicate the details of the problem and the status of any fix that is being put in place to all affected parties.

At minimum, all customers must be notified in game of the disruption to service. If appropriate, the ability for a customer to place a bet should be removed.

Close the Incident

When the problem has been resolved, and monitored for an appropriate amount of time, the incident can be closed. Two things need to happen to close the incident. Firstly, a review should be conducted which includes investigating how the problem arose, the steps taken to solve it and how future similar problems can be avoided. This step forms part of the G Gaming's commitment to Continuous Improvement. Any actions noted in this step should be carried out. It is the Incident Leader's responsibility to ensure that these actions are followed through and where appropriate incorporated into future processes. Secondly, the fact that the problem has been resolved should be communicated to all affected parties.

Some Incidents require a statement to be made to the relevant Regulatory body. As a part of the closing procedure, the Incident should be reviewed and if necessary, a return should be made to the Regulatory body.

Tracking and Management

Known errors, minor bugs or problems

Small errors or minor customer queries will be dealt with via our existing customer service desk which tracks tickets - Freshservice. Where small corrective actions are required, these are tracked on the BAU/Rota Leankit board. The team handling such minor issues consists of the developers on Rota duty for that weekend the Account Managers attending the daily Support stand-up.

This team is also responsible for escalating when several errors have occurred or when a P1 error has arrived. Following the classification procedure above, at this point the CTO or other leader will be notified and an Incident declared.

Incidents

Once an Incident has been declared, its progress through the stages discussed above will also be tracked. For this purpose we use the [Security Incident Management Track](#).

This allows us to track all work relating to the investigation and resolution of that incident. If we identify as part of that incident that further work is required, a project to track that work will be created and linked to that track item.

Every Major Incident will generate a formal report including corrective actions, root cause analysis and recommendations. This may be shared with customers or regulators, depending not he type of Incident. It will be stored in Dropbox and lined to the track.

Personal Data incident

If a security incident is suspected or confirmed to have affected personal data, the Data Protection Officer will be informed at the earliest possible opportunity and take responsibility for any DPA 2018 or GDPR compliance requirements.

Staff are trained on [Reporting information security events \(A.16.1.2\)](#) and [Reporting information security weaknesses \(A.16.1.3\)](#) as part of [Information security awareness, education and training \(A.7.2.2\)](#).

Documents

-  [Internal SLA_G Games.docx](#) Added: 05/03/2022 Added by: [Helen Walton](#) Version: 1.0
-  [Incident Handling Process_G Games.docx](#) Added: 05/03/2022 Added by: [Helen Walton](#) Version: 1.0

Linked work

No Links to display.

A.16.1.2: Reporting information security events

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:24

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 11:43

What we do

Employees and associates are aware of their obligations to report security incidents as part of [Information security awareness, education and training \(A.7.2.2\)](#).

If an information security event occurs, or is believed to have occurred, it must be reported immediately to the CTO, via the support desk or via one of our dedicated Support/Compliance or DevOps channels.

Possible reasons for reporting a security incident include

- Ineffective security control;
- Breach of information integrity, confidentiality or availability expectations;
- Human errors;
- Non-compliances with policies or guidelines;
- Breaches of physical security arrangements;
- Uncontrolled system changes;
- Malfunctions of software or hardware or anomalous behaviour; and
- Access violations.

The support address is monitored during working hours and messages sent to it regarding security events will be flagged as a priority. The CTO or an authorised representative will then create an item on the [Security Incident Management](#) track to capture the work to investigate and as appropriate resolve that incident.

Anonymous reporting

The organisation believes that following its risk assessment and cultural considerations, as well as current size, the need for anonymous reporting outside of the existing channels is very low. Anonymous reporting by customers and other users is not something we anticipate either given the contractual nature and type of services being delivered. However, for anyone wishing to anonymously report security incidents the following applies:

- Ask a trusted friend who is not known to the organisation to ring or email a director of the organisation and share the concerns, without revealing the name of the employee or their relationship.
- The director will then act on that information as per any other security incident.

Customers and other Interested Parties are encouraged to report Security Incidents to their nominated contact, or through the relevant support desk process.

Any reporting externally of Security Incidents e.g. to regulators (under EU GDPR obligations) or other customers and suppliers is done in accordance with [\(A.16.1.4\)](#)

Assessment of and decision on information security events, and [\(A.16.1.5\)](#) Response to information security events.

Linked work

No Links to display.

A.16.1.3: Reporting information security weaknesses

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:25

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2023 at 09:01

What we do

As with reporting security incidents, employees and associates are aware of their obligations to report security weaknesses as part of [Information security awareness, education and training \(A.7.2.2\)](#).

On discovering a security weakness, staff must not attempt to prove that weakness as testing it may be interpreted as a potential misuse of the system and may damage information or the system in question

Suspected security weaknesses must be reported as per the instructions in [Reporting information security events \(A.16.1.2\)](#).

People are able to feedback any incidents including security weaknesses via a range of channels and these include:

- Direct feedback to a member of the Management Review Board;
- Comments on the compliance-isms Slack channel
- Email direct to the e-mail address support@g.games, and
- Contact another member of staff known to them.

All support staff are trained to be aware of security incidents (as part of their general first line triage process) and notify the CTO accordingly in line with the processes described in [Reporting information security events \(A.16.1.2\)](#).

Linked work

No Links to display.

A.16.1.4: Assessment of and decision on information security events

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:25

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:10

What we do

When a security event is created on the Security Incident Management Track [as per \(A.16.1.2\)](#), the first task is to assess the event and then determine a course of action. The full process is described in our Incident Handling Process attached to [Responsibilities and procedures \(A.16.1.1\)](#)

The aim is always to

- Minimise any compromise of the Availability, Integrity or Confidentiality (CIA) of information
- Prevent against further incidents
- Minimise disruption to users of that service
- Consider who needs to be informed; internally, customers, suppliers, regulators e.g. within GDPR and Data Protection Act 2018 requirements.

Security events need to be assessed as follows

- **Security Event** - An action or occurrence that may have (but didn't or hasn't yet) led to information being compromised in terms of its CIA
- **Security Incident** - An action or occurrence that did lead to a compromise in terms of information CIA and can be evidenced to that effect
- **Security Weakness** - A process or flaw in a system that allows a user to compromise the CIA of information held within an information system

As part of that assessment we must also classify the severity and impact of the incident and indicate that within the item tracking that issue.

Once assessed, a lead for responding to that event is nominated and the CTO and any relevant parties required to resolve that event are informed.

If the incident affects customer data, the primary contact for that customer must be informed immediately and their advice sought as to whether any further notification is required.

Any requirement for reporting relevant information security events to [interested parties](#) and any [contact with authorities](#) including customers, suppliers* and regulators** is managed by the Management Review Board, including the CTO as part of its normal operating processes and in accordance with the wider ISMS policies and controls. The DPO takes responsibility for leading on compliance with the Data Protection Act 2018 and GDPR where personal data is affected.

The item is set to a status of Response on the Security Incident Management track. The details of a response to an Information Security Incident are detailed in [Response to information security events \(A.16.1.5\)](#).

* Also in accordance with any specific customer reporting requirements agreed as part of bespoke contracts of major incidents that fall within the GDPR notification for individuals.

**e.g. The Information Commissioner's Office (ICO) as a Supervisory Authority if personal data is affected and is likely to result in a high risk to the rights and freedoms of individuals. Or the UKGC if this is a notifiable event.

Linked work

No Links to display.

A.16.1.5: Response to information security events

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:25

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:12

What we do

During the [Assessment of and decision on information security events \(A.16.1.4\)](#) a lead is assigned in the [Security Incident Track](#) to respond to the security event. They will be responsible for restoring a normal level of security whilst:

- Collecting evidence as soon as possible after the occurrence;
- Conducting information security forensics analysis, as required in line with [Collection of evidence \(A.16.1.7\)](#);
- Escalation, as required internally, with specified customers and if appropriate to the relevant information commissioner as part of the GDPR - and tagged accordingly in the Security Incident Track;
- Ensuring that all involved response activities are properly logged in the track item for later analysis;
- Communicating the existence of the information security incident or any relevant details to the CTO, CEO and CCO for them to inform other internal and external people or organisations with a need-to-know; and
- Dealing with information security weaknesses found to cause or contribute to the incident.

Once the incident is resolved the track item is set to a status of "Review". In accordance with [Learning from information security incidents \(A.16.1.16\)](#) post-incident analysis should take place, as necessary, to identify the source of the incident, the Report be formally presented and stored and any additional reporting be made before the Incident is closed.

Linked work

No Links to display.

A.16.1.6: Learning from information security incidents

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:26

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:14

What we do

As part of our commitment to continual improvement we want to ensure that we learn the lessons of any security incident to help evolve and adapt our ISMS.

The use of the [Security Incident Management track \(A.16.1.2\)](#) allows us to review and filter all major incidents, while analysis of our Tickets in our Support desk allow us to help spot trends and areas for improvement, not only from serious issues but also to examine Failure Demand and its impact on our business. Our process outlined in [Assessment of and decision on information security events \(A.16.1.4\)](#) ensures we are flagging significant events.

Once an incident has been resolved it is set to a status of Review, and the CTO and the lead responder for that incident will discuss any changes required to processes of ISMS policies as a result. Any relevant recommendations will then be put to the Management Review Board for ratification or further discussion as required in line with [9.3](#).

In addition our control to [Demonstrate how nonconformities and corrective actions will be addressed \(10.1\)](#) will be used where required in particular for repeating issues and where audits expose nonconformance or specific customer complaints arise.

Once the review and learning has been completed and agreed by the core team and updates have been made to ISO policies as required, then relevant staff and any other relevant parties must be notified and trained as appropriate in the new/revised policies and process for that area via our process for [Information security awareness, education and training \(A.7.2.2\)](#).

Linked work

No Links to display.

A.16.1.7: Collection of evidence

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:26

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:18

What we do

Where we suspect or know that a security incident may result in legal or disciplinary action, we carry out the following steps:

For digital data on software services we produce and manage

1. Collect the evidence related to the security incident. This may mean examining detailed logs both from the centralised database store (Kibana) or from the transactional data. The collection of evidence will be managed by the Incident Leader and may involve other members of the technical team or the hosting provider if the incident relates to a remote server.
2. Once the evidence has been collected and the Incident Leader is satisfied of its authenticity and integrity it will be uploaded into the relevant place in our software environment and also stored in an encrypted form elsewhere for backup. If the marking of the evidence is considered to be greater than our systems are allowed to hold then we will abide by the prevailing regulations on suitable places where the backup data can be stored.

For digital data on third party systems

1. If the incident took place on a third party application, we would use the tools provided by that application to gather evidence
2. If required, we will liaise with that provider directly to gather more detail.
3. In these cases, the Information/Asset owner for that system will lead the collection of evidence with the support of the CTO as needed.
4. Evidence collected will be stored securely within our software service as guided by the CTO

For physical media and devices

1. Where an incident has occurred involving physical media or processing devices known to result in legal action (e.g.: theft / destruction of data / devices) the relevant authorities must be informed and the collection of evidence, chain of custody etc handled by their specialists
2. Any physical media relating to the incident must be held securely and without interference by the CEO, CTO or a nominated representative thereof. A note of the chain of custody should be maintained to

provide to the relevant authorities

3. Where an issue may result in disciplinary action the evidence must be taken as soon as practical to the CEO, CFO or CTO who will ensure its safe keeping whilst disciplinary proceedings progress.

Regulatory and Legislative obligations

All evidence will be retained in accordance with relevant regulations and legislation as outlined in (A.18.1.1) including but not limited to the GDPR, Data Protection Act (2018) and the Police and Criminal Evidence Act (1984).

Linked work

No Links to display.

A.17. Information Security Aspects of Business Continuity Management

A.17.1 Information security continuity

A.17.1.1: Planning information security continuity

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 01/05/2024 21:10

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 01/05/2024 at 21:10

What we do

Information Security is at the heart of the Business Continuity process within our organisation and the overarching approach to this ISMS is a fundamental part of the business continuity consideration itself. The way the ISMS is designed is to make it iterative, dynamic and evolving as the business continues to evolve and grow, and that informs the business continuity management process too.

The [Business Continuity Plan](#) (BCP) is designed as a dynamic workspace rather than a static document to enable effective collaboration and coordination of work that may continue to evolve in times of crisis or disaster.

Information, assets, risks and policies/controls created throughout the ISMS are done with the intention of understanding interruptions and their impact on the business. Business continuity is designed based on the probability of occurrence taking into account the confidentiality, integrity and availability of the information and assets on the business' ability to continue performing as expected.

As part of the broader risk assessment, events that can cause interruptions to business processes are identified, along with the probability and impact of such interruptions and their consequences for information security. This is already conducted in [\(6.1\): A documented information security risk assessment process](#) and the [Risks and Treatment Plan](#) is an integral part of the BCP itself too.

This covers the business impact assessment that is core to business continuity planning.

The severity of any event is evaluated using the same criteria that we use in our standard SLA - that is by considering the impact on customers, end users and the business.

A **High** priority incident defines any incident which could directly impacting the provision of services as a whole for a confirmed, large number of users. For example, that means that the incident will either be having direct impact on revenue streams and G's reputation and customers.

A **Medium** priority incident defines any incident which could impact a player's experience, but is not affecting the overall experience, revenue sources or reputation. This might mean an issue to G's admin systems which needs to be fixed, but which is not immediately impacting customers. This would include incidents that impact on key staff members since the impact on customers will not be immediate but will soon become apparent.

A **Low** priority incident defines an incident which may only indirectly impact players' experience. Although an impact on G's business operations may seem critical, because of our distributed and remote infrastructure, disasters impacting specific locations will still probably count as low priority unless they directly impact on key members of staff.

Access to the plan in the event of an event

With the BCP held on ISMS.online that in itself helps mitigate any issues about the ability to access the BCP during an event as the service is 'always on' and hosted in the cloud. The plan is accessible to authorised users any location there is internet access. There is very low risk to ISMS itself going down.

Linked work

No Links to display.

A.17.1.2: Implementing information security continuity

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 01/05/2024 21:13

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:26

What we do

Planning information security continuity (A.17.1.1) lays out our approach to business continuity and information security during an unforeseen event. It also includes a business continuity plan that describes:

- a) The management structure in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
- b) The incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security
- c) The documented plans, response and recovery procedures, detailing how the organisation will manage a disruptive event and will maintain its information security to a predetermined level

Specific areas for ISMS include

Server and database redundancy

The 'G Games backup and recovery process' document governs all elements of the Server and Database Redundancy and forms part of our Business Continuity and Disaster Recovery.

IT hardware availability and ease of configuration

The selection of hardware for the CSL datacentre is influenced by the supplier's ability to rapidly replace hardware, in times of emergency. This avoids configuration problems with replacement hardware.

Data and software backups

Regular back up of customer data is made in accordance with the details specified in our plans [A.12.3.1 Information Backup](#). All company documents and data is saved to secure cloud- based solutions.

Communications

G Games relies on internet connectivity and mobile telecommunications to perform its business. In the event that the primary Internet Service Provider is unavailable, G Games will avail itself of the services of another ISP utilising different infrastructure.

This is all implemented through the ISMS contained within this online environment itself.

Other controls in this ISMS describe how as an agile, distributed organisation, using predominately cloud based services, the organisation can cope with a number of business continuity situations with only a minor disruption to service and little or no impact to information security. Such controls include:

- [Teleworking \(A.6.2.2\)](#); and
- [Information backup \(A.12.3.1\)](#)

Linked work

No Links to display.

A.17.1.3: Verify, review and evaluate information security continuity

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 01/05/2024 21:15

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 01/05/2024 at 21:15

What we do

Testing and maintaining the business continuity plan to ensure it is consistent with our information security objectives is done on the basis of the following:

- BCP Audits are planned regularly in line with the audit programme as part of [\(9.2\)](#).
- Spot audits and reviews, including testing staff awareness of information security in relation to business continuity, may be considered by the Management Review Board if it has reason to consider there are risks or issues emerging that have not been previously considered e.g. due to new information (emerging IS threats,) or changes in the organisation (personnel, significant growth etc) or significant changes to service hosting or architecture that may impact information security.
- Reviews of the overall plan itself for ensuring relevance are conducted by the Management Review Board at least once a year to ensure it remains part of an integrated approach to the business and its ability to meet its objectives.

Linked work

No Links to display.

A.17.2 Redundancies. Objective: To ensure availability of information processing facilities.

A.17.2.1: Availability of information processing facilities

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 01/05/2024 21:29

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:30

What we do

As an organisation we build, provide and use cloud-based services for the delivery of our work. These systems have inherent redundancy built into their high-availability, resilient architectures.

Controls where redundancy and resilience are covered elsewhere in this standard include:

- [Capacity management \(A.12.1.3\)](#);
- [Information backup \(A.12.3.1\)](#); and
- [Network controls \(A.13.1.1\)](#).

In addition to the above, the availability of those services can also be determined by:

1. The suppliers availability guarantee and policy on redundancy, which must be considered as meeting our requirements as part of our [Information security policy for supplier relationships \(A.15.1.1\)](#)
2. The availability of a suitable device for using that service. Employees are issued with the assets required for the delivery of their role, or are permitted to use their own equipment in line with our policy for the [Acceptable use of assets \(A.8.1.3\)](#). Where a device is rendered unusable the organisation can issue a temporary device to cover the period of repair or replacement to ensure continued access to systems as needed.
3. The availability of a suitable network to access that service over, This is covered by [Access to networks and network services \(A.9.1.2\)](#) and [Teleworking \(A.6.2.2\)](#).

Linked work

No Links to display.

A.18. Compliance

A.18.1 Compliance with legal and contractual requirements. Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.1.1: Identification of applicable legislation and contractual requirements

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 01/05/2024 21:30

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 26/04/2023 at 08:40

What we do

The applicable legislation, regulation and contractual requirements affecting our organisation are identified and added to the [Compliance Register](#) attached to this Policy. Treatments to ensure compliance are considered and, where appropriate, tied back into ISMS controls. This is regularly reviewed with reminders set against the legislation and offers a better approach towards demonstrating compliance confidence. In the case of G this includes a compliance calendar with automations linked to our database airtable to ensure certificates are renewed appropriately and audits take place with appropriate regularity.

The method for treating risks around applicable legislation, regulation and contractual requirements is documented as part of the organisation's comprehensive approach to risk management expressed in [\(6.1\)](#).

The organisation monitors applicable legislation and reviews it as part of the normal course of its business and as part of the management reviews specified in [\(9.3\)](#). Relevant legislation aspects are discussed where appropriate during Management Review Board meetings in accordance with [\(9.3\)](#) and further action is taken as needed either in the risk area itself, or from the Management Review Board tasking/activity management.

Other contractual requirements are addressed within:

- [Agreements on information transfer \(A.13.2.2\)](#);
- [Confidentiality or non-disclosure agreements \(A.13.2.4\)](#); and
- [Addressing information security in supplier agreements \(A.15.1.2\)](#).
- Service Level Agreement (attached to this policy)

Documents



[SLA-G.docx](#) Added: 05/03/2022 Added by: [Helen Walton](#) Version: 1.0

Linked work

No Links to display.

A.18.1.2: Intellectual property rights

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:28

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:43

What we do

Our intellectual property

The organisation sets out its approach to its own Intellectual Property Rights (IPR) protection in each of the following which are derived from controls set out elsewhere and include:

- [Terms & conditions of employment \(A.7.1.2\)](#)
- [Acceptable use of assets \(A.8.1.3\)](#) – where a breach of IPR is specifically identified as “Unacceptable use”
- [Confidentiality or non-disclosure \(A.13.2.4\)](#)
- Staff and associates will mark information as owned by the organisation where appropriate and protect it including use of copyright statements as appropriate in materials and assets produced by the organisation (e.g. customer proposals, presentation materials, code base)
- Registration of design, patent, trademarks, domain names to the appropriate authorities and following those relevant registration and management practices with records held both in the authority's systems, and the organisation's own system as well
- Ensuring that IPR is documented as an asset in the [Inventory of assets \(A.8.1.1\)](#).
- Ensuring that our contracts and supply agreements with Customers, Partners and Suppliers contain appropriate clauses on our own IP. (See the example supply agreement attached to [A.13.2.4 Confidentiality or non disclosure agreements](#))

Third-party intellectual property

In relation to the IPR of other parties the following apply:

- [Acceptable use of assets \(A.8.1.3\)](#) – where a breach of IPR is specifically identified as “Unacceptable use”

- All staff will comply by the terms of any agreements negotiated by the board whether for customer, supplier or other stakeholders for their IP. These will be documented and held in the relevant account or shared collaboration area in accordance with (A.15.1.2) - note that in some cases our commitments to partners (such as a rights holder) will need to be passed onto our customers or partners via an addendum.
- For generic third-party licences e.g. opensource and proprietary software that is free to use then the person downloading the software needs to be aware of its limitations and obligations (only business oriented software shall be downloaded in accordance with the operating procedures for sourcing software expressed in this ISMS)
- Trial software can be used for evaluation. It does not have to formally documented but users do need to consider the risks based on risk assessment principles documented in the ISMS.
- Any purchased software needs to be registered in the asset register with licence numbers where appropriate
- No third-party software shall be copied without approval or licences to do so and all chargeable software should be sourced using the process outlined in the operating procedure and in accordance with (A.15.1.1).
- Software that still has a value, recovered off devices that no longer require them, is added back into the asset register for reuse
- Internal audits are conducted at planned intervals in accordance with (9.2)

Linked work

No Links to display.

A.18.1.3: Protection of records

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:27

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:49

What we do

Organisation records are kept protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislative, regulatory, contractual and business requirements. This includes:

- All information of value is backed up with the various cloud providers in accordance with our controls for [Information backup \(A.12.3.1\)](#).
- Access to information is granted based on our:
 - [Access control policy \(A.9.1.1\)](#) for access rules;
 - [Inventory of assets \(A.8.1.1\)](#) for asset responsibility; and
 - [Classification of information \(A.8.2.1\)](#).
- Where access to records needs to be controlled with suppliers, customers and other interested parties control is managed through our controls for [Confidentiality or non-disclosure agreements \(A.13.2.4\)](#)

Retention periods

Specific records are kept in line with the following retention policies, managed by the relevant information / asset owner:

Financial statutory & regulatory information	6 years or however long the regulations require if they should change
HR records	for as long as the person is employed, and in accordance with the Data Protection Act, GDPR, Rehabilitation of Offenders Act, Employment Act and for pension, audit & taxation purpose
Information held about customers, suppliers and others such as prospects	in accordance with the Data Protection Act, GDPR, and as required for audit and taxation
General business information for the organisation (e.g. sales collateral, delivery methods etc)	for as long as it has a value in life
Customer data on our software delivered services	for as long as we are required by customers (we don't delete any customer data unless specifically requested to do so - they are able to do that themselves)
Infrastructure critical information (e.g. log files etc)	For as long as required in relation to the investigation of events and incidents. Where log information contains PII this will be reduced to remain compliant with GDPR and DPA.
Game and Transaction Information	Due to the quantity of game data, this is kept accessible to our monitoring and reporting tools for 3 months when it is written to long-term data storage where it can be retrieved and rebuilt following the necessary request or authorisation from the CTO.

Storage of records

The organisation has few paper-based records and wherever possible relies on digital media for its protection of records.

Digital records are stored in a cloud service and protected according to our [Information security policy for suppliers \(A.15.1.1\)](#).

Consideration is given to manufacturers' recommended lifetimes for storage. This is reviewed as required from time to time in accordance with the equipment maintenance activity where information backup policies also apply.

Linked work

No Links to display.

A.18.1.4: Privacy and protection of personally identifiable information

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:28

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:53

What we do

General

The entire purpose of the ISMS is to protect information of any type and all controls contained within the ISMS relate to the protection of personally identifiable information (PII) as much as any other.

Under our classification scheme, PII is classified as "Private" unless it is very basic corporate contact information (e.g. the name and business contact information of a lead contact at a customer etc).

Whether as a data controller (e.g. managing data about staff or customers) or data processor (e.g. processing data for customers about their data subjects) the practices comply with Data Protection legislation for the countries in which we sell and deliver our services; primarily the UK and EU. This also therefore covers GDPR through the Data Protection Act (2018) although we recognise that customers use our products in other countries too.

Staff awareness

All staff handling personal information have awareness of the data protection and privacy principles and ensure personal data should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organisational measures to protect personal information include:

- Data Protection training and awareness during induction with a record held in the employee induction project in line with our [information security awareness, training and education \(A.7.2.2\)](#);
- Updates each year to the Notion page (and communicated using the shared messaging tool; and
- Ad-hoc guidance from time to time by the DPO or other Management Review Board members.

The policy applies to all identifiable personal data held by the company, including on all devices whether for the organisation, its customers, suppliers or other stakeholders.

Applicable policies

Protection of privacy and protection of personal information is supported and reinforced through our:

- [Terms & conditions of employment \(A.7.1.2\)](#);
- [Acceptable use of assets policy \(A.8.1.3\)](#); and
- [Code of Conduct](#).
- Our example Data Processing Agreement is attached to [A.13.2.4 Confidentiality and non disclosure agreements](#)

EU General Data Protection Regulation (GDPR)

The organisation also complies with the EU GDPR for working with EU Citizen data and those countries like the UK which have also committed to adopt the regulation domestically for personal data as well.

In addition to the standard ISO 27001 ISMS controls within this policies and controls environment, it includes a complementary GDPR focused compliance environment* which specifically addresses the detailed requirements of the regulation.

Implementation of specific policies and controls documented elsewhere e.g. right to be forgotten, consent management etc is undertaken within the relevant data subject management system e.g. CRM, customer database etc not within this ISMS.

Documents

 [Data Protection Policy \(GDPR\) v1.0.docx](#) Added: 22/10/2021 Added by: [ISMS Creator](#) Version: 1.0

Linked work

No Links to display.

A.18.1.5: Regulation of cryptographic controls

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:29

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:54

What we do

Cryptographic controls will be used in compliance with all relevant agreements, laws, and regulations.

This is mandated within our [policy on the use of cryptographic controls \(A.10.1.1\)](#)

Linked work

No Links to display.

A.18.2 Information security reviews. Objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

A.18.2.1: Independent review of information security

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:30

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:56

What we do

General

The organisation's entire ISMS is subject to independent review at regular intervals and when changes are made, as part of our commitment to continual service improvement.

All audit activity is coordinated through the [audit project environment](#) with review findings associated to the relevant deliverable in the phase. Other feedback may be taken through the Management Review Board.

Any identified nonconformities or recommendations are logged on the [ISMS Corrective Actions & Improvement Track](#) as per the process described in [\(10.1\): Demonstrate how nonconformities and corrective actions will be addressed](#) which includes actions to:

- Identify the causes of the noncompliance;
- Evaluate the need for actions to achieve compliance;
- Implement appropriate corrective action; and
- Review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.

The Management Review Board will approve and monitor any changes.

Internal audits

- The Management Review Board set out the scope of reviews in the Audit environment in accordance with [\(9.2\)](#).
- The Management Review Board are responsible for planning audits and recruiting independent reviewers for conducting assessments.

Certification Audits

- Selection of an external certification body is managed under our controls for Supplier relationships [\(A.15\)](#) and additionally must be accredited by a recognised authority (e.g. UKAS)
- The selected certification body carries out audits of the ISMS in accordance with the accrediting body's (e.g. UKAS) requirements which include at minimum an annual surveillance audit and a re-certification audit every 3 years.

Customer audits & reviews

- Customers and prospects have the right to conduct independent reviews

Regular review of controls

- All controls are independently reviewed and approved by relevant Management Review Board members as evidenced through the activity approval process of this ISMS.online system management environment.
- Policies are reviewed in accordance with [Review of policies for information security \(A.5.1.2\)](#)

Selection of internal reviewers & auditors

Independent reviewers for more formal audits may be drawn then trained from the following pool:

- Other internal departments
- Associates with relevant skills and experience in the field
- Customers with relevant skills and experience in the field
- Specialist parties e.g. independent security specialists to audit our practices

Review techniques may include one or more of:

- Interviews with management and staff
- Checking records
- Review of security policy documents

Linked work

No Links to display.

A.18.2.2: Compliance with security policies and standards

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:30

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:56

What we do

The [Management Review Board as per \(9.3\)](#) has been established to oversee compliance, and the correct operation of this ISMS.

Where practicable, managers are encouraged to implement automated reporting mechanisms to help them understand that compliance is being maintained (e.g.: automatic notification of backup success, site up-time monitors etc)

Reviews and audits which check compliance are implemented through:

- [Internal audits \(9.2\)](#);
- [Independent review of information security \(A.18.2.1\)](#); and
- Certification audits.

Consequences of non-compliance with policies

Any non-compliance with or breach of policy may lead to investigation and action in line with the organisational [Disciplinary Process \(A.7.2.3\)](#).

Linked work

No Links to display.

A.18.2.3: Technical compliance review

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:31

Statement of Applicability: Applicable - implemented This control is deemed to be applicable based on risk assessment and the control has been implemented.

Categories:

No Categories to display

Added by Helen Walton on 05/03/2022 at 13:58

What we do

General

The organisation's approach to technical compliance checking operates in a similar fashion to [\(A.18.2.2\): Compliance with security policies and standards](#) however any deficiencies or improvements around the work involving development resource will generally be delivered and monitored through the use of the production ticket management system, and customer support case management system.

Many tests for technical compliance are mandated under the regulations by which we hold supplier licences in the various jurisdictions in which we operate - these may include policy audits or regular vulnerability and penetration scanning.

Vulnerability & penetration tests

- Specialist services will be procured in accordance with our controls relating to [Supplier relationships \(A.15\)](#)
- Tests will be conducted in accordance with our controls relating to [Information systems audit controls \(A.12.7.1\)](#)

- Identified vulnerabilities will be recorded on the [ISMS Corrective actions and improvements track](#), prioritised according to risk levels and actioned as appropriate.

Linked work

No Links to display.

Code of Conduct and Social Media Guidelines

Code of Conduct, Social Media Guidelines and Equal Opportunities Policy

Code of Conduct

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:31

Categories:

No Categories to display

Added by Helen Walton on 25/02/2022 at 19:12

Policy

1. Introduction & Vision

G wants to create games that matter to our customers and which our players love.

All of us have one job description: to contribute value to the company and to collaborate to do so.

This Code of Conduct describes G's ethical values and vision. It sets out the principles that are expected of all employees, and, identifies policies that are relevant to the conduct of business.

The requirements of this Code apply to all employees, Board Members and Advisers, along with contractors and consultancies engaged to carry out work for the organisation (hereafter all described as Employees for the purpose of this Code of Conduct).

2. Our values and behaviour

We like to work differently.

1. Just minions

Everyone is a doer, not a manager. We don't have authoritarian hierarchies (natural and evolving hierarchies are fine) but we do believe in expertise and we have high trust in one another. Also-minions are the best characters.

2.Deliver value

There are so many ways in which we can be better.

Better games, better customer service, better systems and processes.... just better.

Everyone who joins us has the opportunity and responsibility to make us better and to choose the work that will make the biggest impact in delivering that value.

3.Collaborate to do so

We also believe that great as everyone may be individually, together we can achieve more than we could alone. To deliver that value, we ask that you collaborate - also - there's nothing more satisfying than working with people you respect.

4.Radical transparency

To make good decisions in the long-term interest of the whole company, people need good information. That's why we believe in radical transparency.Anyone can access any company document, or attend any meeting; all information is available, from financials to salaries to product performance to strategy

We are super open and honest with our staff about all kinds of data and that means you're expected not to share that information outside the company.

3. Principles

Integrity and Honesty

We work in a highly regulated industry. It is essential that as a company we act with integrity and honesty towards ur regulator, our customers and our players. Our employees need to do the same.

We want to celebrate achievements, learn quickly from success and failure and be honest about our strengths and areas for improvement. Employees need to be honest with each other and also look to drive up standards for themselves and others.

We operate in a high performance challenging environment with limited resources however will continue to invest in the careers of our staff, but cannot afford to carry passengers or non performers. Our view is that integrity and honesty also extends to supporting staff to perform well, and having difficult yet honest conversations too when they are required, especially if trust and confidence in delivery falls below acceptable standards.

Objectivity and Openness

Employees should make decisions objectively and wherever possible openly with clear criteria underpinning their decisions in a fair and impartial manner both internally and externally. We have a lot of tools to help with this, from our prioritisation techniques to shared files and working spaces. Use them and continue to check up on how we change things on notion.

Responsibility and Accountability

Employees are responsible for their actions and accountable for their decisions and behaviours to their colleagues, customers and partners.

4. Business Conduct

We will provide a professional, safe and healthy environment for the workforce demonstrated through its efforts to achieve and retain recognised accreditations including but not limited to International Standards and the Health & Safety at Work Act 1974.

We will protect the integrity, availability, and confidentiality of all personal and corporate information held by us in either manual or electronic form as evidenced in gaining standards such as ISO 27001 along with other relevant certifications.

We are committed to equality and inclusion in all business, HR and technical policies, controls and operating procedures - see [Equal Opportunities Policy](#)

We respect the right to privacy and data protection within the Data Protection Act 2018 and, GDPR and the Human Rights Act 1998. When staff are absent for long periods (outside holidays) or there is a disaster, we reserve the right to contact staff at home or access their work email, other systems and office held files.

The Employees' Commitment

All Employees must respect the principles in this Code and set out elsewhere in the relevant policies of the ISMS. It is the personal responsibility of every Employee to act in accordance with our policies - many of which are necessary for our existence as a regulated and licensed business. If employees are unable to do so for whatever reason they must let a colleague know and ask for help.

All policies can be found in the relevant controls areas and communications groups environments. Employees have a responsibility to ensure that they understand the objectives incumbent upon them and all the policies

All employees have a duty to their employer not to act in a manner that prejudices the health and safety of another employee, customer, partner or anyone else. Employees should also raise concerns to a Director if they suspect fraud, bribery or any other abuse of a position held by work colleagues.

All employees also have responsibilities around preventing gambling harm in each aspect of their jobs, from design to customer service. There are also Anti Money Laundering and Wistleblowing policies which are relevant to our specific industry that employees must comply with.

All employees must avoid engaging in activities that are likely to breach that contract or bring disrepute or damage upon the organisation, even where such conduct occurs outside of work. Employees must not do anything while on or off duty that could harm the organisation's reputation and/or lead to criminal charges against them. This includes verbal or written communications and general work practices, including email and social media activity that breaches policies, legislation or regulation.

Employees should be aware that failure to adhere to the principles contained in this Code, and/ or any policy, legislation or regulation applicable to their employment may be considered a disciplinary matter, and under certain circumstances can bring about instant dismissal.

Raising concerns

Employees are often the first to realise that there may be something wrong within a company. G Gaming views whistleblowing as a positive act that can make a valuable contribution to the efficiency and long-term success of the company. It is not disloyal to colleagues or the company to speak up.

It is essential that everyone working for the organisation feels able to raise any concerns they have about the way business is being conducted in a manner that is simple, effective and confidential. We will ensure employees feel able to raise concerns without fear of any reprisals being taken against them including making available no blame review sessions and anonymous reporting as set out in the relevant policy areas.

Concerns can be raised about any aspect of the organisation's activities, e.g. fraud or financial impropriety, harassment, bullying, discrimination; health and safety, decisions, actions, conduct or communications that are

unlawful, in breach of policies or in significant breach of our values and vision.

For full details, please see our Whistleblowing Policy.

Linked work

No Links to display.

Social Media Guidelines

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:37

Categories:

No Categories to display

Added by Helen Walton on 08/05/2024 at 09:36

Policy

Purpose

Our organisation embraces the potential of social media as a vehicle to inform, excite, share and engage with audiences both B2B and B2C.

Definition of social media

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as Twitter, Facebook and LinkedIn. Social media also covers blogs and video- and image-sharing websites such as YouTube and Flickr.

Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow these guidelines in relation to any social media that they use.

Use of social media for the purpose of work

We encourage employees to make reasonable and appropriate use of social media websites as part of their work. It is an important part of how the organisation communicates with its customers and promotes its services.

Employees must be aware at all times that, while contributing to the organisation's social media activities, they are representing the organisation. Staff who use social media as part of their job must adhere to the following rules.

Practical Guidelines

Employees should adopt a common sense approach and use the same safeguards as they would with any other form of communication about the organisation in the public sphere, whilst adhering to the Code of Conduct. These safeguards include:

- Making sure that the communication has a purpose and a benefit for the organisation;
- Adding value to any conversation or forum. Do not just post sales related messages or broadcast in a spam like manner. If you can't add value then just observe and wait until you can;
- Anything done on social media needs to be compliant with the ISMS and our Code of Conduct;
- That you are responsible for what you publish.

Any communications that employees make in a professional capacity through social media must not:

- Bring the organisation into disrepute, for example by:
 - Criticising or arguing with customers, colleagues or rivals;
 - Making defamatory comments about individuals or other organisations or groups; or
 - Posting images that are inappropriate or links to inappropriate content;
- Breach confidentiality, for example by:
 - Revealing trade secrets or information owned by the organisation;
 - Giving away confidential information about an individual (such as a colleague or customer contact) or organisation (such as a rival business); or
 - Discussing the organisation's internal workings (such as deals that it is doing with a customer/client or its future business plans that have not been communicated to the public);
- Breach copyright, for example by:
 - Using someone else's images or written content without permission;
 - Failing to give acknowledgement where permission has been given to reproduce something; or
- Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
 - Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
 - Using social media to bully another individual (such as an employee of the organisation); or
 - Posting images that are discriminatory or offensive or links to such content.

Using social media with our brands

- Only authorised employees and associates should use the organisation's branded social media accounts
- Any registration in business forums, sites and related vehicles should be done with the organisation name or relevant work email addresses and real names.
- Business sites that encourage profiles should be completed with relevant details to help promote and inform about our brands and your role.

- Sign up for notifications and news as you see fit, sharing that back with colleagues in the organisation as required to help make better business decisions.
- Please consider the use of social media generally as being 'public' from an information classification perspective so be careful what you post, even in direct messages.
- Except for content on specified systems that is generally considered 'commercial in confidence' please do not send or share sensitive 'commercial in confidence' information over other social media.
- Be aware that gambling is a sensitive topic and others may occasionally launch personal and emotional attacks on those who work in the industry - strive to be polite at all times, but feel free to disengage and to ask for help from Directors on how or whether to respond to comments.
- For those speaking or writing on regulatory topics, be sensitive to how outsiders (especially the media or anti-gambling groups) might choose to interpret comments and be very careful about wording that might suggest anything relating to addiction, appealing to younger players or suggesting the gambling increases wellbeing or 'life changing' events.

Social media in your personal life

We recognise that many employees make use of social media in a personal capacity. While they are not acting on behalf of the organisation, employees must be aware that gambling is a sensitive area in which some groups and media outlets may actively monitor for posts which are seen to be careless about gambling related harm.

Employees are allowed to say that they work for the organisation, which recognises that it is natural for its staff sometimes to want to discuss their work on social media. However, the employee's online profile (for example, the name of a blog or a Twitter name) should not contain the organisation's name.

If employees do discuss their work on social media (for example, giving opinions on their specialism or the sector in which the organisation operates), they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer" or "The postings on this site are my own and don't necessarily represent the organisation, positions or strategy."

Any communications that employees make in a personal capacity through social media must not:

- Bring the organisation into disrepute, for example by:
 - Criticising or arguing with customers, colleagues or rivals;
 - Making defamatory comments about individuals or other organisations or groups; or
 - Posting images that are inappropriate or links to inappropriate content;
- Breach confidentiality, for example by:
 - Revealing trade secrets or information owned by the organisation;
 - Giving away confidential information about an individual (such as a colleague or customer contact) or organisation (such as a rival business); or
 - Discussing the organisation's internal workings (such as deals that it is doing with a customer/client or its future business plans that have not been communicated to the public);
- Breach copyright, for example by:
 - Using someone else's images or written content without permission;
 - Failing to give acknowledgement where permission has been given to reproduce something; or

- Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
 - Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
 - Using social media to bully another individual (such as an employee of the organisation); or
 - Posting images that are discriminatory or offensive or links to such content.

Use of social media in the recruitment process

Unless it is in relation to finding candidates (for example, if an individual has put his/her details on social media websites for the purpose of attracting prospective employers), managers should conduct searches, either themselves or through a third party, on social media only when these are directly relevant to the applicant's skills or claims that he/she has made in the recruitment process. For instance:

- A prospective employee might claim that he/she has used social media in his/her previous job (for example, as a publicity tool); or
- A prospective employee's social media use may be directly relevant to a claim made in his/her application (for example, if he/she runs a blog based around a hobby mentioned in his/her CV or a skill in which he/she claims to be proficient).

There should be no systematic or routine checking of prospective employees' online social media activities, as conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision. This is in line with the organisation's equal opportunities policy.

Disciplinary action over social media use

All employees are required to adhere to this policy. Employees should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal.

Linked work

No Links to display.

Equal Opportunities Policy

Assigned to: Helen Walton

Days estimated: 0.0

Days taken: not set

Due: not set

Status: Completed

Approved by Helen Walton on 08/05/2024 09:37

Categories:

No Categories to display

Added by Helen Walton on 25/02/2022 at 19:24

Policy

Introduction

We value and celebrate the diversity that exists in our workforce and our committed to creating a working environment in which everyone has the opportunity to fully take part. We aim to develop, promote and deliver our employment, volunteering and training opportunities, without discrimination. G Gaming, hereinafter known as the Company, is committed to maintaining the highest possible standards of conduct to ensure our compliance at all times; this policy aims to maintain these high standards alongside our other policies.

Principles

The Company is fully committed to eliminating discrimination in recruitment, training and working conditions, and to promoting equality of opportunity and treatment.

We believe that encouraging diversity of ideas, thinking and experience leads to better ways of working and better business results. We're committed to building a diverse workforce and encouraging an inclusive culture. This covers all areas of diversity, including race, sex, gender identity, age, marital status, sexual orientation, or any other reason not related to job performance or prohibited by applicable law.

Compliance with this policy should also ensure that employees do not commit unlawful acts of discrimination.

Striving to ensure that the work environment is free of harassment and bullying and that everyone is treated with dignity and respect, is an important aspect of ensuring equal opportunities in employment.

Why do we have an Equal Opportunities policy?

An effectively implemented Equal Opportunities Policy will help us to:

- Provide an environment conducive to the promotion of fair and equal opportunities to all employees
- Ensure fair treatment for all job applicants and existing employees
- Ensure fair treatment for all others with whom we have contact e.g. contractors and customers
- Make the best possible use of our existing and potential workforce
- Improve employment practices and staff morale
- Attract, develop and retain the good quality employees who are essential for achievement of our business objectives
- Avoid unlawful or unfair discrimination as noted in the Equality Act 2010

We believe that it is in everyone's best interests to ensure that the experience, talents and skills available throughout its organisation are considered when employment or development opportunities arise.

What has it got to do with me?

Equal opportunities impose rights and responsibilities for every employee. Everyone has a right to fair and dignified treatment. This means that no-one will be discriminated against nor harassed. Every employee has an obligation to ensure fair and dignified treatment. The contribution of everyone will be valued and everyone will be treated purely on their merits. Everyone must act fairly, within our stated policies and the law. Failure to do so may lead to disciplinary action.

The Law

A number of laws exist to ensure equality and diversity are recognised and protected, these include the following in the United Kingdom:

- Equality Act 2010
- Equal Pay Act 1970
- Human Rights Act 1998
- Rehabilitation of Offenders Act 1974
- Part-time Workers Regulations 2000
- Fixed-term Employees Regulations 2002
- Agency Workers Regulations 2010
- Gender Recognition Act 2004
- Civil Partnership Act 2004

As the Company operates internationally, particular attention should be paid to the laws of each jurisdiction to ensure that we are legally compliant at all times with each jurisdictions' own laws.

It is unlawful to discriminate directly or indirectly in recruitment or employment because of:

- Age
- Disability
- Sex
- Gender reassignment
- Pregnancy
- Maternity
- Race (which includes colour, nationality and ethnic or national origins)
- Sexual orientation, or because someone is married or in a civil partnership
- Religion or belief

These are known as "protected characteristics".

Discrimination after employment may also be unlawful, e.g. refusing to give a reference for a reason related to one of the protected characteristics.

Employees should not discriminate against or harass a member of the public in the provision of services or goods. It is unlawful to fail to make reasonable adjustments to overcome barriers to using services caused by disability. The duty to make reasonable adjustments includes the removal, adaptation or alteration of physical features, if the physical features make it impossible or unreasonably difficult for disabled people to make use of services. In addition, service providers have an obligation to think ahead and address any barriers that may impede disabled people from accessing a service.

Types of unlawful discrimination

Direct discrimination is where a person is treated less favourably than another because of a protected characteristic. An example of direct discrimination would be refusing to employ a person because of their sexual orientation.

In limited circumstances, employers can directly discriminate against an individual for a reason related to any of the protected characteristics where there is an occupational requirement. The occupational requirement must be crucial to the post and a proportionate means of achieving a legitimate aim.

Indirect discrimination is where a provision, criterion or practice is applied that is discriminatory in relation to individuals who have a relevant protected characteristic (although it does not explicitly include pregnancy and maternity, which is covered by indirect sex discrimination), such that it would be to the detriment of people who share that protected characteristic compared with people who do not, and it cannot be shown to be a proportionate means of achieving a legitimate aim.

Harassment is where there is unwanted conduct, related to one of the protected characteristics (other than marriage and civil partnership, and pregnancy and maternity) that has the purpose or effect of violating a person's dignity; or creating an intimidating, hostile, degrading, humiliating or offensive environment. It does not matter whether or not this effect was intended by the person responsible for the conduct.

Associative discrimination is where an individual is directly discriminated against or harassed for association with another individual who has a protected characteristic (although it does not cover harassment because of marriage and civil partnership and, according to guidance from the Government and Acas, pregnancy and maternity).

Perceptive discrimination is where an individual is directly discriminated against or harassed based on a perception that he/she has a particular protected characteristic when he/she does not, in fact, have that protected characteristic (other than marriage and civil partnership, and pregnancy and maternity).

Victimisation occurs where an employee is subjected to a detriment, such as being denied a training opportunity or a promotion because he/she made or supported a complaint or raised a grievance under the Equality Act 2010, or because he/she is suspected of doing so. However, an employee is not protected from victimisation if he/she acted maliciously or made or supported an untrue complaint. There is no longer a need for a complainant to compare his/her treatment with someone who has not made or supported a complaint under the Equality Act 2010. For example, if a blind employee raises a grievance that the employer is not complying with its duty to make reasonable adjustments, and is then systematically excluded from all meetings, such behaviour could amount to victimisation.

Failure to make reasonable adjustments is where a physical feature or a provision, criterion or practice puts a disabled person at a substantial disadvantage compared with someone who does not have that protected characteristic and the employer has failed to make reasonable adjustments to enable the disabled person to overcome the disadvantage.

Equal opportunities in employment

We will avoid unlawful discrimination in all aspects of employment including recruitment, promotion, opportunities for training, pay and benefits, discipline and selection for redundancy.

Person and job specifications will be limited to those requirements that are necessary for the effective performance of the job. Candidates for employment or promotion will be assessed objectively against the requirements for the job, taking account of any reasonable adjustments that may be required for candidates with a disability. Disability and personal or home commitments will not form the basis of employment decisions except where necessary.

We will consider any possible indirectly discriminatory effect of its standard working practices, including the number of hours to be worked, the times at which these are to be worked and the place at which work is to be done, when considering requests for variations to these standard working practices and will refuse such requests only if the organisation considers it has good reasons, unrelated to any protected characteristic, for doing so. We will comply with obligations in relation to statutory requests for contract variations. We will also make reasonable adjustments to standard working practices to overcome barriers caused by disability.

Customers, suppliers and other people not employed by the organisation

We will not discriminate unlawfully against customers using or seeking to use goods, facilities or services provided by the organisation.

Employees should report any bullying or harassment by customers, suppliers, visitors or others to a Director who will take appropriate action.

Your Responsibilities

Every employee is required to assist the organisation to meet its commitment to provide equal opportunities in employment and avoid unlawful discrimination.

Employees can be held personally liable as well as, or instead of, the organisation for any act of unlawful discrimination. Employees who commit serious acts of harassment may be guilty of a criminal offence.

Acts of discrimination, harassment, bullying or victimisation against employees or customers are disciplinary offences and will be dealt with under the organisation's disciplinary procedure. Discrimination, harassment, bullying or victimisation may constitute gross misconduct and could lead to dismissal without notice.

Grievances

If you consider that you may have been unlawfully discriminated against, there are a number of different people you can speak to including any of the Directors.

The duty of confidentiality does not apply if:

- There has been a breach of the law
- There is a risk of harm to the individual or to others.
- The disclosure is in the context of legal or disciplinary procedures.

We will take any complaint seriously and will seek to resolve any grievance that it upholds. You will not be penalised for raising a grievance, even if your grievance is not upheld, unless your complaint is both untrue and made in bad faith.

This does not affect your right to make a complaint to an employment tribunal. Complaints to an employment tribunal must normally be made within three months, beginning with the act of discrimination complained of.

Monitoring and review

This policy will be monitored periodically by the organisation to judge its effectiveness and will be updated in accordance with changes in the law. In particular, the organisation will monitor the ethnic and gender composition of the existing workforce, and of applicants for jobs (including promotion) and the number of people with disabilities within these groups, and will review its equal opportunities policy in accordance with the results shown by the monitoring. If changes are required, the organisation will implement them.

Information provided by job applicants and employees for monitoring purposes will be used only for these purposes and will be dealt with in accordance with the Data Protection Act 1998.

Documents



[Diversity and Equal Opportunities Policy .docx](#) Added: 25/02/2022 Added by: [Helen Walton](#) Version: 1.0

Linked work

No Links to display.

ISO 27001 Policies & Controls

To-dos

Description	Assigned to	Set by	Status	Due date
Review the Activity 'A.8.1.4: Return of assets'	Helen Walton	Helen Walton	Open	08/11/2024
Review the Activity '10.2: Continual improvement'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '10.1: Nonconformities and corrective actions'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '9.3: Management review'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '9.2: Internal audits'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '9.1: Performance evaluation'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '8.1 - 8.3: Planning and control'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '7.5: Documented information'	Helen Walton	Helen Walton	Open	07/08/2024
NB - new standards apply from 2025	Jakub Szerszen	Helen Walton	Completed	07/08/2024
Review the Activity '7.1 - 7.4: Resources'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '6.2: Information security objectives'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '6.1.3: Statement of Applicability'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '6.1: Risk assessment process'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '5.3: Roles and Responsibilities'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '5.2: Information security policy'	Helen Walton	Helen Walton	Open	07/05/2025

Description	Assigned to	Set by	Status	Due date
Review the Activity '5.1: Leadership and commitment'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '4.4: Establish, implement and maintain an ISMS'	Jakub Szerszen	Helen Walton	Open	07/05/2025
Review the Activity '4.3: Scope'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '4.2: Interested parties'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity '4.1: External and internal issues'	Helen Walton	Helen Walton	Open	07/05/2025
Review the Activity 'A.18.1.1: Identification of applicable legislation and contractual requirements'	Helen Walton	Helen Walton	Open	01/05/2025
Review the Activity 'A.17.2.1: Availability of information processing facilities'	Helen Walton	Helen Walton	Open	01/05/2025
Review the Activity 'A.17.1.3: Verify, review and evaluate information security continuity'	Helen Walton	Helen Walton	Open	01/05/2025
Review the Activity 'A.17.1.2: Implementing information security continuity'	Helen Walton	Helen Walton	Open	01/05/2025
Review the Activity 'A.17.1.1: Planning information security continuity'	Helen Walton	Helen Walton	Open	01/05/2025
Review the Activity '5.3: Roles and Responsibilities'	Helen Walton	Helen Walton	Completed	20/02/2025
Review the Activity 'A.17.1.1: Planning information security continuity'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.1.1: Information security requirements analysis and specification'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.13.2.4: Confidentiality or non-disclosure agreements'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.13.2.3: Electronic messaging'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.2.2: System change control procedures'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.2.1: Secure development policy'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.1.3: Protecting application services transactions'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.2.7: Outsourced development'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.2.6: Secure development environment'	Helen Walton	Helen Walton	Completed	26/04/2024

Description	Assigned to	Set by	Status	Due date
Review the Activity 'A.14.2.5: Secure system engineering principles'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.2.4: Restrictions on changes to software packages'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.2.3: Technical review of applications after operating platform changes'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.3.1: Protection of test data'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.14.2.9: System acceptance testing'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.16.1.4: Assessment of and decision on information security events'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.16.1.3: Reporting information security weaknesses'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.16.1.2: Reporting information security events'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.16.1.1: Responsibilities and procedures'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.17.1.1: Planning information security continuity'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.16.1.7: Collection of evidence'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.16.1.6: Learning from information security incidents'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.16.1.5: Response to information security events'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.18.1.1: Identification of applicable legislation and contractual requirements'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.17.2.1: Availability of information processing facilities'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.17.1.2: Implementing information security continuity'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.18.1.5: Regulation of cryptographic controls'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.18.1.4: Privacy and protection of personally identifiable information'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.18.1.3: Protection of records'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.18.1.2: Intellectual property rights'	Helen Walton	Helen Walton	Completed	26/04/2024

Description	Assigned to	Set by	Status	Due date
Review the Activity 'Code of Conduct'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.18.2.3: Technical compliance review'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.18.2.2: Compliance with security policies and standards'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.18.2.1: Independent review of information security'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'Equal Opportunities Policy'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'Social Media Guidelines'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity '6.1.3: Statement of Applicability'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity '4.1: External and internal issues'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'Confirmation of who should access this environment, when and how, their roles, including how access to information is controlled and updated'	Helen Walton	Helen Walton	Open	26/04/2024
Review the Activity 'A.15.2.2: Managing changes to supplier (and other important delivery relationships) services'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.15.2.1: Monitoring and review of supplier services (and other important delivery relationships)'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.17.1.3: Verify, review and evaluate information security continuity'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.15.1.3: Information and communication technology supply chain'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.15.1.2: Addressing security within supplier (and other important relationship) agreements'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.15.1.1: Information security policy for supplier (and other important) relationships'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.8.1.2: Ownership of assets'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.8.1.1: Inventory of assets'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.6.1.3: Contact with authorities'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity '6.1: Risk assessment process'	Helen Walton	Helen Walton	Completed	26/04/2024
Review the Activity 'A.12.4.3: Administrator and operator logs'	Helen Walton	Helen Walton	Completed	21/04/2024

Description	Assigned to	Set by	Status	Due date
Review the Activity 'A.6.1.1: Information security roles and responsibilities'	Helen Walton	Helen Walton	Completed	28/03/2024
Review the Activity 'A.9.4.2: Secure log-on procedures'	Helen Walton	Helen Walton	Completed	22/02/2024
Review the Activity 'A.7.3.1: Termination or change of employment responsibilities'	Helen Walton	Helen Walton	Open	17/01/2024
Review the Activity 'A.6.1.2: Segregation of duties'	Jakub Szerszen	Helen Walton	Completed	17/01/2024
Review the Activity 'A.6.1.1: Information security roles and responsibilities'	Helen Walton	Helen Walton	Completed	22/11/2023
Review the Activity 'A.5.1.2: Review of the policies for information security'	Helen Walton	Helen Walton	Completed	15/11/2023
Review the Activity 'A.5.1.1: Policies for information security'	Helen Walton	Helen Walton	Completed	17/01/2024
Review the Activity '10.2: Continual improvement'	Helen Walton	Helen Walton	Completed	22/11/2023
Review the Activity '10.1: Nonconformities and corrective actions'	Helen Walton	Helen Walton	Completed	23/11/2023
Review the Activity '9.3: Management review'	Helen Walton	Helen Walton	Completed	22/11/2023
Review the Activity '9.2: Internal audits'	Helen Walton	Helen Walton	Completed	15/11/2023
Review the Activity '9.1: Performance evaluation'	Helen Walton	Helen Walton	Completed	17/01/2024
Review the Activity '8.1 - 8.3: Planning and control'	Helen Walton	Helen Walton	Completed	10/01/2024
Review the Activity '7.5: Documented information'	Helen Walton	Helen Walton	Completed	10/01/2024
Review the Activity '6.1: Risk assessment process'	Helen Walton	Helen Walton	Completed	19/01/2023
Review the Activity '5.3: Roles and Responsibilities'	Helen Walton	Helen Walton	Completed	16/11/2023
Review the Activity '5.2: Information security policy'	Helen Walton	Helen Walton	Completed	17/01/2024
Review the Activity '5.1: Leadership and commitment'	Helen Walton	Helen Walton	Completed	17/01/2024
Review the Activity '4.4: Establish, implement and maintain an ISMS'	Jakub Szerszen	Helen Walton	Completed	17/01/2024
Review the Activity '4.4: Establish, implement and maintain an ISMS'	Cheryl Jones	Helen Walton	Completed	10/01/2024

Description	Assigned to	Set by	Status	Due date
Review the Activity '4.3: Scope'	Helen Walton	Helen Walton	Completed	08/11/2023
Review the Activity '4.2: Interested parties'	Helen Walton	Helen Walton	Completed	19/01/2024
Review the Activity 'A.6.1.1: Information security roles and responsibilities'	Helen Walton	Helen Walton	Completed	12/12/2023
Check versioning appears on exports	Helen Walton	Helen Walton	Completed	
Set up KPIs that can be viewed here - start recording results.	Jakub Szerszen	Helen Walton	Completed	30/12/2022
Review and Confirm prior to Internal Audit	Helen Walton	Helen Walton	Completed	30/11/2022
Review the Activity 'Upload your copy of ISO 27001 here for reference'	Helen Walton	Helen Walton	Open	21/06/2023
Review the Activity '4.3: Scope'	Helen Walton	Helen Walton	Completed	09/06/2023
Review the Activity 'A.14.2.8: System security testing'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.11.1.6: Delivery and loading areas'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.9.4.3: Password management system'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.9.1.2: Access to networks and network services'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.11.2.5: Removal of assets'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.11.2.4: Equipment maintenance'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.11.1.6: Delivery and loading areas'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.11.1.5: Working in secure areas'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.11.1.2: Physical entry controls'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.11.1.4: Protecting against external and environmental threats'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.11.1.3: Securing offices, rooms and facilities'	Helen Walton	Helen Walton	Completed	26/04/2023
Review the Activity 'A.8.1.3: Acceptable use of assets'	Helen Walton	Helen Walton	Completed	26/04/2023

Description	Assigned to	Set by	Status	Due date
Review the Activity 'A.9.2.6: Removal or adjustment of access rights'	Natasha Mockett	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.15.2.2: Managing changes to supplier (and other important delivery relationships) services'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.15.2.1: Monitoring and review of supplier services (and other important delivery relationships)'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.17.1.3: Verify, review and evaluate information security continuity'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.15.1.3: Information and communication technology supply chain'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.15.1.2: Addressing security within supplier (and other important relationship) agreements'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.15.1.1: Information security policy for supplier (and other important) relationships'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.8.1.4: Return of assets'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.8.1.2: Ownership of assets'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.8.1.1: Inventory of assets'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.6.1.3: Contact with authorities'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.6.1.2: Segregation of duties'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.6.1.1: Information security roles and responsibilities'	Helen Walton	Natasha Mockett	Completed	30/09/2022
Review the Activity 'A.14.2.7: Outsourced development'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.1.3: Protecting application services transactions'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.2.1: Secure development policy'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.2.2: System change control procedures'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.13.2.3: Electronic messaging'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.13.2.4: Confidentiality or non-disclosure agreements'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.1.1: Information security requirements analysis and specification'	Helen Walton	Dan Rough	Completed	03/03/2023

Description	Assigned to	Set by	Status	Due date
Review the Activity 'A.16.1.2: Reporting information security events'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.16.1.3: Reporting information security weaknesses'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.16.1.4: Assessment of and decision on information security events'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.2.9: System acceptance testing'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.3.1: Protection of test data'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.2.3: Technical review of applications after operating platform changes'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.2.4: Restrictions on changes to software packages'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.2.5: Secure system engineering principles'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.14.2.6: Secure development environment'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.18.1.5: Regulation of cryptographic controls'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.17.1.2: Implementing information security continuity'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.17.2.1: Availability of information processing facilities'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.18.1.1: Identification of applicable legislation and contractual requirements'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.16.1.5: Response to information security events'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.16.1.6: Learning from information security incidents'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.16.1.7: Collection of evidence'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.17.1.1: Planning information security continuity'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.16.1.1: Responsibilities and procedures'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'Social Media Guidelines'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'Equal Opportunities Policy'	Helen Walton	Dan Rough	Completed	03/03/2023

Description	Assigned to	Set by	Status	Due date
Review the Activity 'A.18.2.1: Independent review of information security'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.18.2.2: Compliance with security policies and standards'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.18.2.3: Technical compliance review'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'Code of Conduct'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.18.1.2: Intellectual property rights'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.18.1.3: Protection of records'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.18.1.4: Privacy and protection of personally identifiable information'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '10.2: Continual improvement'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.5.1.1: Policies for information security'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '9.1: Performance evaluation'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '9.2: Internal audits'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '9.3: Management review'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'A.5.1.2: Review of the policies for information security'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '10.1: Nonconformities and corrective actions'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '8.1 - 8.3: Planning and control'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '7.5: Documented information'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '7.1 - 7.4: Resources'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '6.2: Information security objectives'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '6.1.3: Statement of Applicability'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '6.1: Risk assessment process'	Helen Walton	Dan Rough	Completed	03/03/2023

Description	Assigned to	Set by	Status	Due date
Review the Activity '5.3: Roles and Responsibilities'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '5.1: Leadership and commitment'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '5.2: Information security policy'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '4.3: Scope'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '4.2: Interested parties'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity '4.1: External and internal issues'	Helen Walton	Dan Rough	Completed	03/03/2023
Review the Activity 'Confirmation of who should access this environment, when and how, their roles, including how access to information is controlled and updated'	Helen Walton	Dan Rough	Completed	03/03/2023
changes to dev environment section?	Dan Rough	Helen Walton	Completed	
specific to games?	Dan Rough	Helen Walton	Completed	
review @dan players vs operators for tokens?	Dan Rough	Helen Walton	Completed	
Update diagram?	Dan Rough	Helen Walton	Completed	
no idea	Dan Rough	Helen Walton	Completed	
Review this - no idea	Dan Rough	Helen Walton	Completed	
create standing agenda item on management review board 'check audit log'	Jakub Szerszen	Helen Walton	Completed	
ship audit log	Dan Rough	Helen Walton	Completed	
add in server spin up etc	Dan Rough	Helen Walton	Completed	03/03/2022
Discuss proof of process following	Dan Rough	Helen Walton	Completed	
Discuss proof of process following	Jakub Szerszen	Helen Walton	Completed	
Discuss proof of process following	Natasha Mockett	Helen Walton	Completed	
finish listing the process documents	Natasha Mockett	Helen Walton	Completed	

Description	Assigned to	Set by	Status	Due date
finish listing the process documents	Dan Rough	Helen Walton	Completed	
Leaves checklists	Natasha Mockett	Helen Walton	Completed	04/03/2022
Access audit	Natasha Mockett	Helen Walton	Completed	04/03/2022
Separate list of accounts	Natalie Millett	Helen Walton	Completed	04/03/2022
Add a shot of checklist and kickoff agenda?	Jakub Szerszen	Helen Walton	Completed	04/03/2022
Review the Activity 'Making the template documentation work for your organisation and its stakeholders'	Dan Rough	Cheryl Jones	Open	29/10/2022
Attach your standard terms here having made sure they address the requirements of the standard and are fit for purpose.		ISMS Creator	Completed	
Attach your standard terms having made sure they address the requirements of the standard and are fit for purpose.		ISMS Creator	Completed	
Amend the info sec policy document to include references for your organisation		ISMS Creator	Completed	