
Mitratech
Policies and Procedures
v. 1.7

Table of Contents

1.	Information Security Policy	3
2.	User Management Policy	18
3.	Human Resources Roles and Responsibilities	22
4.	System Access Rights Policy	25
5.	Financial Accounting Procedures	28
7.	Business Continuity and Disaster Recovery	32
8.	Backup Procedure	36
9.	Document Control	38

1. Information Security Policy

1.1 Our Principles

Information belonging to or held by the Company, whether personal or non-personal (“Company Information”) is a valuable asset.

Failure to protect these assets leads to their unauthorised access, use, disclosure and destruction. **Adequate protection** of these assets from unauthorised access, use, disclosure and destruction reduces this risk.

Just like any other valuable assets belonging to an individual, such as precious jewellery which is usually deposited in a safe deposit box for safe-keeping – Company Information needs to be adequately protected from thieves or fraudsters.

Inadequate security leads to or may potentially lead to a number of implications for the Company as well as for its customers, which include financial losses, judicial proceedings against the Company, loss of reputation and trust; temporary or permanent ban on data processing issued by the competent authorities if personal information is unlawfully disclosed or processed;

Effective Information Security is a financial investment for the Company. We deem it of utmost importance to ensure that Company Information is secured in such a way that any risk of threats and vulnerabilities is significantly reduced and any expected financial loss or damages resulting from such threats and vulnerabilities is also diminished.

Information Security requires an **evaluation of risks** by assessing the threats and vulnerabilities to the information and ensuring that the Company has the necessary procedures and controls in place to preserve this information in line with **confidentiality, integrity and availability**.

1.2 Security risk assessment

Risk of threats and vulnerabilities to the Company Information can never be fully eliminated. An element of risk however remote is always present.

Risks can however be significantly reduced – by carrying out an **information security risk assessment**.

The Company has: (i) evaluated the current state of its infrastructure, (ii) compiled an inventory of all its assets; and (iii) identified the processes used for accessing the Company Information held in its systems. From the information gathered, risks have been identified, quantified, prioritised and action mitigation controls have been determined and implemented to protect against and reduce risks.

The controls covered by this Policy reduce the risks to an acceptable level for the business.

The Company monitors its risk mitigation plan periodically and performs annual security risk assessments to address any changes in the risk levels or security requirements¹.

¹ See “Monitoring and Compliance Section”

1.3 Access controls

1.3.1 User Management

All access to Company Information, resources and services as well as physical access shall be restricted and controlled. Access to system documentation and software applications shall be restricted. Access to logs, personal data, business sensitive information and to intellectual property (“IP”) shall be strictly restricted, assigned on a need-to-know basis and controlled according to risk assessments and relevant law.

All Users shall be assigned access rights based on the **need-to-know** access control principle. Access rights shall be assigned, audited, and removed through an access control process ensuring that access to Company Information, whether personal or non-personal, resources and services is allowed only on need-to-know or need-to-use basis.

Users shall only be provided with access to the company premises, information, resources, networks, network services and other services which they have been specifically authorized to use. The assessment of the level of access to grant a particular User shall be based on the following factors: risk assessments including any risks associated to: - insufficient confidentiality, integrity, and availability of information; insufficient traceability of the use of the resources; breaches of privacy; violation of immaterial rights. The role of the User and the nature of the role shall also be factored in.

Users shall be required to sign their contract of employment or for the provision of services in the case of third party staff members and sub-contractors which shall contain adequate confidentiality provisions and provisions related to data protection, prior to being provided with any access rights. In the event that the sub-contractor/third party staff member is an organization, any agreement must be signed by its legal representatives. The employees of that organization might be asked to sign a separate non-disclosure agreement and/or data controller-processor agreement prior to being granted access rights.

1.3.2 New Starters, Movers and Leavers

Access rights for new Users shall be determined, and provided in accordance with our policy on “User Management” above.

Users who move cross-functionally, change duties or employment status within the Company shall be immediately removed of their old access rights, if they no longer require the same level of access and granted new access rights based on the need-to-know principle. These changes are to be logged and retained by the Tech department that manages the information security for the company. Users who resign or are released by the Company shall have all their physical, IT, and any other access rights terminated prior to physically exiting the Company premises. The Company will ensure that it has a process in place to ensure that the Users’ accounts will be disabled on all systems where they have their accounts on the last day of their employment or on the day on which their contract terminates, whichever the case may be. Access can only be re-enabled upon approval from the Chief Technology Officer.

A list of all leavers must be provided to the IT Department prior to the last day of employment/expiration of the contract. If a User's contract or employment is being terminated by the Company for HR reasons, his/her account must be disabled before or during the exit interview.

Each User shall be given an exit interview in order to collect keys, cell phones and other equipment and to sign any documents or contracts which might be required. Subject to the termination of the User's employment or contract for HR reasons, once these actions are performed, the account of the User is immediately terminated and deactivated.

1.3.3 Restricted Physical Access & Controls

Certain areas both within the Company offices and outside the main offices ("Premises") are considered more security sensitive than others, such as the server locations.

Physical access to the server location centre is limited to access on a **need-to-know** basis. Only a limited number of authorised employees and other representatives of the Company and of the Malta Gaming Authority ("MGA"), when requested or when necessary, will be granted access to the Company servers. Unaccompanied access to the equipment rooms is not allowed.

Authorisation levels and access rights to our offices and server rooms are administered and approved by our Tech department.

Physical access to the Company's offices has been controlled by means of the following **measures**:

- Minimum entry points;
- Identification badge;
- Biometrics (fingerprint)
- Locks on doors and cabinets.

The Company Premises will be **monitored** with security cameras all times and the footage shall be retained for a limited defined period as provided in our Retention Policy, after which it shall be properly disposed of in accordance with this Policy² (see "Disposal"). The security cameras will cover the entire area of the premises, with the exception of the restrooms and other areas prohibited by law from being monitored. Appropriate standard operating procedures will be applied to all security camera equipment and applications to ensure effective and ethical management of the equipment as well as appropriate maintenance of the footage by authorised users. The Company will ensure that the below measures are taken in relation to the installation of the security cameras within the Premises:

- All security cameras will be installed in secure areas within the Company Premises;
- Easily visible signs shall be placed in all monitored areas;
- Access to the security camera equipment and footage will be restricted to authorised users;

² See "Disposal"

- The footage will be processed and retained in accordance with data protection legislation and will only be accessed in the event of a security investigation.

The Company acknowledges that the security cameras may also capture and record the movements of its employees during working hours. To this effect, the Company will ensure that all employees will be adequately informed and will obtain the necessary consents from the same for the processing (capture) of their images.

The Company shall regularly monitor the security camera equipment to ensure that each security camera is still appropriate for the task as well as to effect any changes to the positioning of the same following any modifications carried out to the areas/building.

All employees and visitors authorized to access the Company Premises must display prominently at all times an identification badge and access card issued by the Company, which displays:

- the individual's full name;
- the employing company;
- the type of identification (employee, contractor, visitor);
- a photograph (solely in relation to employees).

Tracking and monitoring of physical access to the Premises is provided by:

- security cameras;
- the verification of visitors' identity and entry into the premises;
- the logging of exit and entry details from the biometrics (fingerprint);
- monitoring of network access.

All our employees are trained and fully aware:

- To report any suspicious activity to their manager;
- To escort their visitors throughout the duration of their visit;
- To courteously challenge any employee or visitor if the badge is not displayed;
- To shred all confidential documents upon completion of the task;
- To authorize and record all movement of material entering and leaving the premises;
- To forbid tail-gating;
- Not to permit photos taken in processing facilities;
- To keep their identification badges in a safe place when they are not within the Company Premises;
- To report lost or presumably stolen identification badges immediately in accordance with the Company's escalation procedure;

1.3.4 Visitor Access

Visitor access to the Company's Premises is strictly controlled.

Only designated authorised key personnel have physical access to the server room, as authorised by the Tech department (main resp. is the CTO).

In order for a visitor to be granted access to any server room, they must be identified with proper official identification to ensure that they have the correct authorization. When such visitors have been allowed entry to the site, at least one employee will escort the visitor during the whole visit. In no circumstances will the visitor be allowed to be present at the data centre without supervision. All visitors are assigned a visitor card (badge/access card) to identify them at any time when inside the facility so that they can be distinguished from the data centre employees.

Visitors will have to report to the reception area of the Company's offices to gain entry. Entry to the reception area from outside is controlled by the receptionist. Entry within the offices beyond the reception area is not possible until a visitor's badge is issued. Issuing and logging of the visitor is performed with the receptionist. On leaving the company, visitors are logged out and the badges are collected.

1.3.5 Remote Access for Users

We promote teleworking within our organization. Remote access provides a similar experience to "working from the office": once connected the User is placed on the corporate network via a virtual private network ("VPN") connection using the approved VPN client and appropriate authentication (two-factor).

Remote access to Company Information by Users may be allowed after applying the adequate protective measures in accordance with the results from the Company's information classification or risk assessment. Remote access of each User is approved by the Tech department through the person responsible, stated in 4. System Access Rights Policy

Remote access is also restricted to authorised members and representatives of the MGA, when requested or when necessary.

1.3.6 Session Time-Out

All sessions shall be automatically shut down after 15 minutes of inactivity. Users must input their login details and reconnect via VPN, if connecting remotely.

1.3.7 Password Management

All Users must input a unique User ID and a password (two-factor authentication) in order to be able to access the Company's systems.

1.3.8 Employees' Password Management

Temporary passwords are assigned to Users upon commencement of employment. Users are advised to change this password immediately after the first login to one of their choice.

The Company raises awareness internally on the importance of **good and effective password management**, in particular it stresses the importance of the following:

- Passwords allowing broad access to Company information systems must be different to passwords used for personal accounts;
- Blank-field passwords are not allowed by the Company and its systems are designed to automatically reject any blank field passwords.
- Passwords must contain not less than 8 characters.
- A combination of upper and lowercase and alphanumeric characters and at least one special character;
- If an account or password is suspected to have been compromised, Users shall be required to change their passwords immediately and report the matter in accordance with our Incident Response Policy;
- Inactive accounts (no activity for 3 months or over) and accounts of employees who have terminated their employment with the Company shall be disabled;
- Users should opt for passwords which are not easy to guess or which can be easily associated with them such as nicknames, pet names, known interests, common dictionary words, birthdays.
- Passwords cannot be reused.
- Users are responsible for their passwords and must refrain from disclosing the same and any other login details to anyone including family members. Users shall also refrain from writing passwords down or store them online or on their devices.
- The User will be locked out from the system after six failed access attempts (such as inputting of wrong password). The lockout duration will last for 30 minutes or until the system administrator re-enables the User ID, whichever is the earlier.
- Passwords must be re-entered after 30 minutes of inactivity.

1.3.9 Device and Equipment Management

- Desktop, Portable Devices, Storage Media and Peripheral Equipment

The Company may provide desktop as well as mobile devices including laptops, mobile phones, tablets and storage media (such as USB pen drives, DVD/CD, etc) to employees and other Users whose role requires them (collectively “Devices”). Users are able to access internal e-mail, calendars and contacts, as well as other resources and applications available on the internal network from mobile phones, tablets and laptops, as if they are accessing these from their desktops.

Each of these hardware Devices, including peripheral equipment such as fax machines, printers and photocopiers, has the ability to create, receive, store, access or share Company Information.

Security measures for peripheral equipment include:

- Photocopiers, printers and fax machines that store or transmit confidential or sensitive information shall be placed in secure locations and monitored.
- All documents containing confidential or sensitive information shall immediately be cleared from printers, copiers and fax machines.

Portable Devices present a special risk purely due to their mobility and as a result are vulnerable to theft (consequently to data theft) and loss. Therefore, the Company recognises the importance and necessity of applying extra security measures to protect the Company Information stored within those Devices.

Users who are granted access to the Company's network or information systems shall adequately secure their Devices from unauthorized access.

Best practice security measures implemented by the Company include the following safeguards:

- Devices should be locked when unattended;
- A password system must be used or PIN code must be activated on the Device to protect the contents of the same;
- Devices must be protected at all times from heat, cold, water, smoke, dust, physical damage and magnetic interference;
- Devices should not be used in public places to avoid situations where passers-by might have visibility of the contents of the display;
- USB Mass Storage Devices must be removed from the Device when not in use, stored securely and returned to the Tech department when no longer required;
- The Company should be informed immediately if the Device is misplaced, stolen or presumed stolen. This would enable the Company to take the necessary immediate security measures to protect the Company Information stored on the Device, including remote Data Wipe-Out³.

The Company provides local and network storage within the organization to easily manage and store files, thus reducing the use of removable storage Devices for most day-to-day tasks.

³ See "Remote Data Wipe"

Given the large amount of information which removable storage media Devices can store, the Company has defined **additional controls** to minimise risks.

The Company only allows the use of removable storage media Devices in instances when large amounts of information need to be shared internally or externally. In these cases the following requirements need to be met:

- Approval needs to be obtained from the Tech department;
- Data can only be stored in a Company provided storage device;
- Personal data must be stored according to any data protection legislation

The Company does not encourage the use of online file hosting services to reduce risks. Users shall be unable to download such applications onto the company-owned Devices as this functionality will be disabled.

1.3.10 Usage of Personal Devices

Employees who are not supplied with Company-owned mobile handsets, tablets or laptops might require remote access to the Company email account, calendar and contacts. Authorization must be requested from the Tech department to connect their personal mobile devices to the company servers.

The following requirements apply:

- Users are only able to access internal e-mail, calendar and contacts. Any other service cannot be accessed through personal devices;
- Adherence to the best practice security measures⁴;

1.3.11 Remote Data Wipe

Although there are circumstances where Users can access Company Information through their personal Devices, any Company Information created, received or stored within that personal Device remains the property of the Company at all times. To ensure adequate protection of Company Information, the Company will require the User to acknowledge this Policy on use of personal devices as well as specifically consent to the fact that once the User no longer requires access to Company Information from the personal Device, all Company Information, namely emails (corporate email account) and work calendar will be remotely wiped-out, before access is provided. The User shall also acknowledge that whilst the Company shall use its best efforts to ensure that only Company Information will be erased from the personal Device, it cannot exclude the possibility of erasing personal data stored within the Device, apart from Company Information. The User shall be fully aware that this might happen and is responsible to ensure that s/he regularly backs-up his/her personal

⁴ See: "Desktop, Portable Devices, Storage Media and Peripheral Equipment"

content stored on the Device. The User shall also acknowledge that s/he will not hold the Company responsible, if this happens.

If the Device whether personal or Company-owned, is stolen, misplaced or presumed stolen, the user is obliged to inform the Company immediately and without undue delay. The Company shall immediately initiate a “Lock” and Remote Data Wipe of the Device.

1.4 Disposal

1.4.1 Disposal of Media and Equipment

The disposal of electronic records stored on media, computer equipment, and computer software can create information security risks. These risks are related to the potential unauthorized disclosure of Company Information, violations of software license agreements, and unauthorized disclosure of intellectual property that could be stored on storage media, computer equipment, and computer software.

This Policy governs the requirements of secure disposal of media containing Company Information, as well as the secure disposal of Company Information stored on other equipment, by establishing a process which ensures the secure removal of sensitive data or protected information from storage media or from the equipment, prior to disposal.

This Policy covers all fixed and removable storage devices and all equipment such as Devices owned by the Company. This includes, but is not limited to: magnetic media (including fixed disks, magnetic tape, floppy, and other removable drive disks), optical disks, non-volatile memory devices (including memory sticks and cards or USB memory storage), PDAs, laptops, desktops. Any storage devices or Devices currently available, or which may become available in the future due to new technology, are also covered by this Policy.

- The Company shall assign the responsibility of disposal to a member of its staff with a suitable level of authority who shall authorize the disposal and shall be responsible to maintain a full inventory of all equipment including media which has been marked for disposal;
- The Company will opt for the appropriate disposal methods upon taking into consideration the security vulnerabilities associated with each method;
- All electronic Devices and media equipment, including storage media in personal computers and other hardware containing Company Information, must be degaussed (demagnetised) prior to disposal so that the data will not be retrieved and reused. The sanitisation methods used will depend on the type of media and the intended disposal of the media.
- Non-functioning and/or non-writable media containing Company Information must be physically destroyed if degaussing or other sanitisation is determined to be inadequate.

- Disposal of media requires authorisation and tracking by the CTO, responsible for the information security.
- Where possible, destruction will be performed on-site.
- Damaged media and drives cannot be sent for repair and must be physically destroyed.
- All methods of media disposal shall be in compliance with information security best practices.

The Company reserves the right to either internally re-deploy Devices especially desktops, laptops and mobile phones or donate/sell them to third parties outside the organisation, instead of destroying them. The Company shall however make sure that all Company Information including any software and any other residual data are properly deleted from the Devices prior to the re-deployment, donation or sale.

1.5 Safeguarding of Applications

1.5.1 Application Security

- Privacy and Security are integral components of software development life-cycle. All applications developed by the Company must have documented security analysis included in the specification and design documentation, following a security risk assessment. A privacy impact assessment must also be carried out in the early stages of development to cater for any privacy risks prior to the deployment of the application ("**Privacy By Design**").
- All applications must be developed according to security best practices and international standards (such as ISO 27001 "Information Security Management"; ISO 27002 "Information technology- Security techniques-Code of Practice for Information Security Controls" and any other international standards which may be applicable).
- Any modification to core functionality must be peer reviewed.
- Any application modifications with security and/or privacy implications must be signed-off by the CTO and CEO before a release. Notwithstanding the security and privacy impact assessments, all applications must still be tested for common security and privacy weaknesses before deployment and no application should be released containing known security and/or privacy vulnerabilities.
- All developers must be familiar with common application security and privacy weaknesses.
- No test or debugging functionality can be present in final product builds.
- Management interfaces must only be reachable through the internal network and never exposed publically, even if restricted to a set of addresses or if protected by a password.

- Application documentation must include Security controls and Security test plans.
- Each application is integrated with static source code analysis nightly build.
- All applications must be classified in order of required security level.
- Critical applications are subject to an annual audit plan.
- Third-party components in our developed applications fall inside scope.

1.6 Safeguarding of equipment

The Company has the right to monitor any and all aspects of its phone and computer systems for security purposes as well as monitor and/or access communication logs, including without limitation those related to phone (company-owned), corporate email accounts or internet communications upon reasonable grounds of suspicion of any unlawful activity by any User or upon any threat, whether immediate or otherwise to the security of the Company Information. The Company shall however make sure that all Users are informed of the Company's policy on monitoring of communications.

1.7 Network Protection

1.7.1 Network Hardware

All network hardware is cloud based and managed by AWS (Amazon) and will follow their strict security policy. See systems overview document.

1.7.2 Network Systems

The Company's network systems are protected by firewalls, passwords and authentication requirements, VPNs and encryption as well as digital keys for all authorised employees. To safe guard player sessions system communicating with during sessions must use HTTPS: secure communication protocol.

1.7.3 Emails

The Company's email system shall not be used for unlawful purposes, namely it shall not be used for the creation or distribution of any illegal, disruptive or offensive messages, including spam. Subject to the above provision on the right by the Company to monitor aspects of its systems, the privacy of the content of emails will be respected. There might be exceptional circumstances (such as upon reasonable grounds of suspicion of any unlawful activity by any User or upon any threat, whether immediate or otherwise to the security of the Company Information) where the Company may require access to the Users' corporate emails and content for investigation purposes.

The Company acknowledges that Users might use a reasonable amount of the Company's resources for personal emails (non-work related emails) and this is deemed acceptable by the Company. Personal emails shall be saved in a separate folder from work related email.

Users must check all information they communicate to others via email to ensure that Company Information is not transmitted unintentionally and should refrain from sending internal emails to external parties.

Users should report any suspicious emails (such as suspicion that an email contains a virus or if an email has been received from an unknown source) to the Tech department.

1.8 Antivirus/Antimalware Protection and other Perimeter Controls to Minimise Threat of Intrusion

The Company shall implement the necessary perimeter network controls to prevent or minimise the risk of penetration of the Company's network from the outside. Some of the measures taken by the Company include: antivirus applications, firewalls, VPNs and encryption. The Company shall also use intrusion detection and intrusion prevention systems.

1.8.1 Antivirus/Antimalware solutions

The Company shall install the necessary antivirus/antimalware protection within its infrastructure to protect critical desktop and server operating systems against viruses, spyware, rootkits and other security threats. It also ensures that the firewall is active and working efficiently to protect against network layer threats. Incoming and outgoing emails shall be scanned for viruses and any email attachments shall be scanned for spyware or adware applications. The Company shall ensure that the antivirus/antimalware protection will run continuously and will automatically update virus definitions and software as well as generate audit logs.

Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, bacteria, worm, Trojan horse, or the like).

Suspected viruses should be reported immediately to the Tech department. The Company shall immediately inform the relevant authorities as soon as malicious code or suspicious codes are discovered in the system. The Company shall also take the necessary immediate steps to ensure that the malicious code does not affect the Company's systems and the Company Information stored therein.

1.8.2 Encryption and Authentication

The Company understands the importance of ensuring effective system security by implementing the necessary and adequate security controls and preventing unauthorised access to, use and disclosure of Company Information. An important measure is the encryption of information.

The exchange of confidential or sensitive information, as classified in our Information Classification

policy via email or otherwise, shall be encrypted. TLS encryption is used for emails and HTTPs for back-office and SSH for remote communication with servers.

The Company acknowledges that encryption alone is not sufficient. Whilst encryption ensures that the information remains confidential, it cannot authenticate the information, and this might lead to the risk of repudiation. The Company shall implement authentication measures such as digital signatures to minimise this risk as described above.

1.9 Information Asset Management

1.9.1 Clear Desk/Screen Policy

The Company's clear desk/screen policy complements the best practice security measures mentioned above⁵.

1.9.2 Clear Desk Policy

- Desks and workstations should be clear of all confidential and sensitive information, when the Users are away from their desk or office. Paper and storage media should be stored in lockable cabinets or any other lockable storage when not in use, especially outside working hours;
- Where lockable storage is not available, office doors must be locked if left unattended. At the end of each working day all Company Information should be removed from the workstation/desk and stored in a locked area;
- Confidential and sensitive information, when printed, should be cleared from printers immediately. Where possible printers with a 'locked job' facility should be used;
- Any visit, appointment or message books should be stored in a locked area when not in use;
- The reception desk should be kept as clear as possible at all times.

1.9.3 Clear Screen Policy

- Desktop and laptops must not be left logged on when unattended and must be password protected. The Windows security lock should be set to activate when there is no activity for a short pre-determined period of time and should be password protected for reactivation;
- Computer screens must be strategically positioned, away from the view of unauthorized persons.

1.10 Retention

Retention of Company Information by the Company can be required from a legal, regulatory or business perspective. Company Information shall be retained in accordance with the Company Information Retention Policy.

⁵ As listed under "Device and Equipment Management"

Company Information shall not be retained for a period longer than necessary, unless the Company has a specific purpose to retain certain documents for a longer period. Reasons for longer retention can be found in the Retention Policy.

1.11 Backup

- Server systems must be regularly backed-up using a standard backup methodology. Backup media must regularly be transferred and stored securely on or off-site.
- Sensitive and confidential Company Information must be encrypted when backed up and be capable of authorised decryption for at least as long as required for legal or regulatory compliance.
- Backup systems must be periodically tested to ensure that the procedure works as expected.
- Backup media must be archived for the retention period established in the Retention Policy.

1.12 Information Classification

Company Information has varying degrees of sensitivity and criticality. The higher the value of the Company Information and the higher the sensitivity, the greater the security required. Company Information must first be valued. Once a value has been given, a classification can be established and a corresponding security level can be identified and implemented.

In order to determine the asset value, the following factors shall be taken into consideration: - the level of sensitivity and confidentiality of the information; the associated business impact, the potential financial implications and the business needs for sharing or restricting information.

The Company has defined the following information classifications for data and documents.

- Confidential;
- Sensitive;
- Public

Confidential: Company Information classified as Confidential must be highly secured and remain private. If disclosed, Confidential Company Information would significantly impact the business or data subjects.

Sensitive: Company Information marked as Sensitive should be adequately secured. Sensitive information can be shared internally but not externally.

Public: Company Information which can be shared externally.

2. User Management Policy

2.1 Email Usage

Email communication is one of the most important means of communication throughout the business world. Messages can be transferred quickly and conveniently across the internal network and globally via the public Internet. Conducting business via email has its risks. Emails can be insecure, particularly when transmitted outside the internal network and can be intercepted and read in transit, potentially changed and sent to the intended recipient, without the latter being aware of any alteration. It is vital therefore that the Company takes all the necessary measures to protect emails from unauthorized access and ensure that emails have not been modified or tampered with in any manner by unauthorized parties whilst making sure that the mail servers remain available for business purposes at all times.

Best practice security measures implemented by the Company, include the following safeguards on acceptable email usage:

- All emails must be encrypted. No confidential/sensitive information, can be transmitted particularly over the internet, unless it is first encrypted by an encryption system approved by Information Security Department;
- Users cannot create, send, forward or store emails with messages or attachments that might be illegal or considered offensive, sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive or any other illegal, unethical or unauthorized purpose.
- Users must refrain from committing or binding the Company towards a third party, in any manner whatsoever, including through purchase or sales contracts, job offers or price quotations, unless authorisation in writing from senior management has been obtained.
- No emails can be sent without the standard corporate email disclaimer, which is automatically appended to emails sent externally outside the organisation. Users must not interfere with or remove this disclaimer;
- Limited personal use of the corporate email systems is permitted at the discretion of the management provided always that it is incidental and occasional, and does not interfere with business. There are no expectations of privacy: all emails traversing the corporate systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees.
- Emails cannot be used in ways that could be interpreted as representing or being official public statements on behalf of the Company, unless the User is explicitly authorized by senior management to make such statements;
- Users cannot send emails or other messages from anyone else's account or in their name (including the use of false 'From:' addresses). Upon obtaining the necessary authorisation from

the manager, a secretary may send emails on the manager's behalf but must always include the following wording "for and on behalf of" the manager (manager's name) beneath his or her name;

All Users must:

- check all information they communicate to others via email to ensure that Company Information is not transmitted unintentionally and should refrain from sending internal emails to external parties.
- not disclose potentially sensitive information in "out of office" messages, unnecessarily.
- report any suspicious emails to the Information Security department. Emails on the corporate IT systems are automatically scanned for malicious software, spam and unencrypted proprietary or personal information. Unfortunately, the Company cannot guarantee however that this process is 100% effective (e.g. compressed and encrypted attachments may not be fully scanned).
- intercept, divert, modify, delete, save or disclose emails to unauthorized parties, except when specifically authorised by management or where necessary for IT system administration purposes.
- External/third---party email services (commonly known as "webmail") should not be used for business purposes.

Subject to the provisions of the Information Security Policy, the Company has the right to monitor as well as access any and all aspects of corporate email accounts or internet communications upon reasonable grounds of suspicion of any unlawful activity by any User or upon any threat, whether immediate or otherwise to the security of the Company Information, for investigation purposes. The Company shall however make sure that all Users are informed of the Company's policy on monitoring of communications and shall use its best endeavours to ensure that the privacy of the email content will be respected.

2.2 Password Management

A poorly chosen password may compromise the Company's entire corporate network.

This policy states the minimum requirements for passwords for the Company. Further information on the company's password management can be found in the Information Security Policy.

2.3 Employees' Password Management

Temporary passwords are assigned to Users upon commencement of employment. Users are advised to change this password immediately after the first login to one of their choice.

The Company raises awareness internally on the importance of **good and effective password management**, in particular it stresses the importance of the following:

- Passwords allowing broad access to Company information systems must be different to passwords used for personal accounts;
- Blank-field passwords are not allowed by the Company and its systems are designed to automatically reject any blank field passwords.
- Passwords must contain not less than 8 characters.
- A combination of upper and lowercase and alphanumeric characters and at least one special character;
- If an account or password is suspected to have been compromised, Users shall be required to change their passwords immediately and report the matter in accordance with our Incident Response Policy;
- Inactive accounts (no activity for 3 months or over) and accounts of employees who have terminated their employment with the Company shall be disabled;
- Users should opt for passwords which are not easy to guess or which can be easily associated with them such as nicknames, pet names, known interests, common dictionary words, birthdays.
- Passwords cannot be reused.
- Users are responsible for their passwords and must refrain from disclosing the same and any other login details to anyone including family members. Users shall also refrain from writing passwords down or store them online or on their devices.
- The User will be locked out from the system after six failed access attempts (such as inputting of wrong password). The lockout duration will last for 30 minutes or until the system administrator re-enables the User ID, whichever is the earlier.
- Passwords must be re-entered after 30 minutes of inactivity.

2.4Employment Termination

Employees may be employed by the Company on both definite and indefinite contracts. All employees must be registered with the Employment Training Corporation (“ETC”) and must be approved by the MGA.

When a contract of employment is terminated the Company shall, within three (3) days from the date of termination, notify the ETC by means of a termination form.

A notice shall also be sent to the MGA informing the Authority that the employee in question is no longer employed with the Company within three days

With regards to access rights, employees who move cross-functionally, change duties or employment status within the Company shall be removed of their old access rights and granted new access rights based on the need-to-know access principle. These changes are to be logged and retained by the Information Security Department.

A notice shall also be sent to the MGA informing the Authority that the employee in question has changed duties within the Company to be sent within three days

Employees who resign or are released by the Company shall have all their physical, IT, and any other access rights terminated prior to physically exiting the Company premises. Each employee shall be given an exit interview in order to collect keys, cell phones and other equipment and to sign any documents or contracts which might be required. Once these actions are performed, the account of the employee is immediately terminated and deactivated.

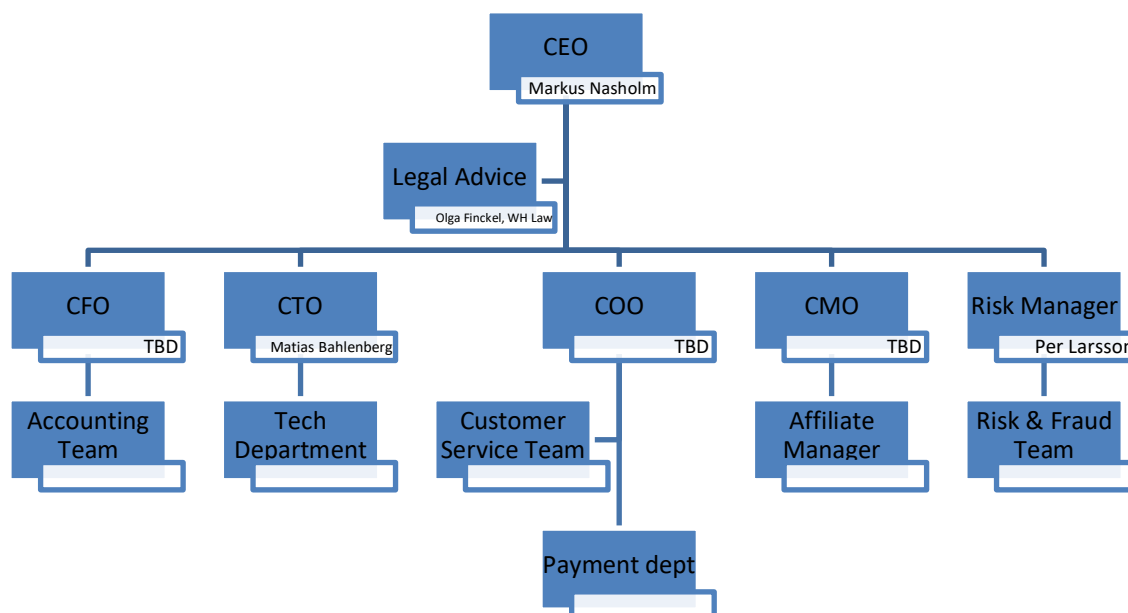
Periodic checks of access rights are done to ensure that no terminated user is still enable in the system

3. Human Resources Roles and Responsibilities

3.1 Organisational Setup

Mitrtech is organised to handle all gaming operations in Malta such as client support, finance handling, campaign and client communication strategies and execution.

Below is an organisation chart meant to reflect the company organisation 6 months after go live.



3.2 Role Descriptions

The Key Functions for B2B licensee are the following:

a) The Chief Executive Role – Markus Näsholm

This person shall be responsible for the day to day management and administration of the Company. They shall also oversee all legal affairs and ensure that the company is compliant with any applicable laws. The person would be responsible for the licensee's finances except for the payment of taxes and fees due in terms of the law.

b) The day to day gaming operations of the Licensee – Markus Näsholm

This position is responsible for developing and implementing a strategic plan to grow the gaming revenue and devise and implement the product content. Apart from this, such a person would be responsible for planning the yearly budget. Such a person is also entrusted with maintaining and managing customer and supplier relationships.

c) Compliance with the licensee's obligations- Per Larsson

As a compliance officer for the company, this person would have to oversee the ongoing day-to-day responsibility for the operations. Furthermore, this person would also be required to develop and maintain compliance policies and procedures. Above all, this person would have to ensure that all the necessary due diligence would have been obtained. All these responsibilities would ultimately emanate from the licence or licences issued by the Authority.

d) The Administrative and Financial and risk strategies of the licensee – Markus Näsholm

e) Marketing and Advertising – Markus Näsholm

The chief Marketing Officer would be responsible for creating and managing effective plans focused on customer acquisition, conversion and retention. They would also oversee all marketing activities and contribute to product development strategies. Furthermore, this person would also need to forecast the performance of the business.

f) The Legal Affairs of the Licensee – WH Partner

This includes but is not limited to contractual arrangements and dispute resolution. This person would have to ensure that the licensee is always fully compliant with the everchanging legislative requirements of this jurisdiction. Furthermore, this person would have to be able to identify and mitigate any risks that the licensee would be susceptible to.

g) Adherence to applicable legislation relating to data protection and privacy – Per Larsson

The Data Protection Officer shall be responsible for ensuring that the organisation meets with the requirements under the EU's General Data Protection Regulations (GDPR).

h) The Technological affairs of the licensee – Matias Bahlenberg

This person would need to establish and oversee the company's technological vision and all its necessary aspects. This includes but is not limited to the management of the back-end and control system holding essential regulatory data.

i) The Network and Information Security of the Licensee – Matias Bahlenberg

The key person is required to oversee all system designs and changes in system architecture and also needs to plan and implement all needed documentation for internal and external systems of staff.

j) Internal Audit – Per Larsson

This person would be responsible for implementing effective internal auditing measures. This would ensure that the company is in line with the relevant regulations. This person would also ensure that regular audits are carried out, and the results of which are analysed and discussed with the rest of the company.

A key person shall notify the Authority, not later than 3 working days from the date of occurrence if:

- a) Any circumstance arises which may render him not fit and proper to carry out such key function.
- b) Any circumstance which arises in relation to a licensee for which he performs a key function, which the licensee is obliged to report.
- c) Any circumstance arises in relation to a licensee for which he performs a key function which may render the licensee incapable of meeting one or more of its obligations related to the function which the key person performs for that licensee.
- d) His resignation or dismissal from exercising a key function
- e) Any other circumstance which the key person believes the Authority should be aware of.

The Authority will be notified by no later than three (3) working days following resignation, dismissal or changes to persons performing one or more key functions.

4. System Access Rights Policy

4.1 About

Access control Policy lays down rules and procedures for the allocation of the rights and authorisation for accessing the data, applications and systems, and specifies the responsibilities in their implementation. The rules and procedures allow for the control of access to the information assets of the Company and reduce the possibility of unauthorised access, which may result in disclosure, loss or corruption of data.

Terms of accesses must comply with safety requirements, while enabling smooth functioning of business services at the same time. The establishment of rules is based on the categorisation of information, the applicable legislation and the contractual obligations which relate to the protection of access to information and services.

Failure to comply with the policy by the employees constitutes professional misconduct. In case of violation, the employee shall be liable and a disciplinary action might be taken against him in accordance with the applicable labour legislation.

4.2 Access rights

All system accesses are logged and these logs are available for possible audit. They will be reviewed periodically by the CTO, Matias Bahlenberg,

System access is given only on a need-to-know basis.

In a case that a third party (other than suppliers with access) needs to access the System, they need permission from CTO Matias Bahlenberg and in case of physical access also KO. This permission will be limited to certain time frame.

Access to key systems and networks is controlled physically and logically. This means that unauthorized personnel will not have access to those areas.

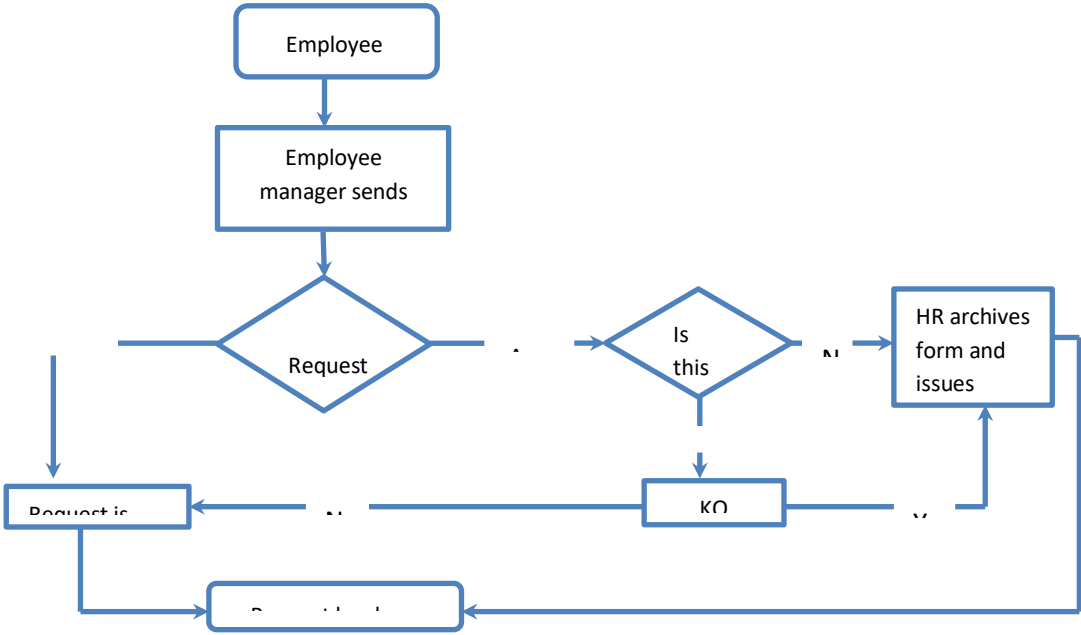
4.3 Procedure detailing the assignment of access rights

Each Manager has by default permission to initiate system authorization requests for their personnel if they themselves have system access. Every request for this access must be validated by CTO, Matias Bahlenberg.

These authorisation requests will be handled by sending appropriate form via email and emails with requests/approvals will be cc'ed to a separate account, so it will be possible to review all history.

If the request is approved, the approving authority will create an account on a corresponding part of the System.

Procedure for access is detailed below.



4.4 System access rights level per job designation

The access to the system is being controlled by AIM (Access and Identity Management) in AWS. Each registered user has been assigned to a security group (role) for proper access in each environment. The authentication is being performed by personal access keys via SSH.

Mitrtech Operations Limited addresses system access rights in the following ways:

Job Description	Full Access	Read Only Access	No Access
CEO			X
CTO		X	
CFO			X
Systems Administrator	X		
Compliance and Legal		X	
CMO			
DPO		X	
Senior Developer			
Junior Developer			
Support	(X) Dep. On work descr	X	
Third Party			X

4.5 Physical access rights

The purpose of having a physical access policy is to ensure that no unauthorized individual can be given access to the sites that are used for production. The limited access to the site will eliminate the risk of malicious actions being taken on the physical servers, and also allow traceability if an error occurs. As the solution is cloud based, only AWS have physical access.

Job Description	Access with Supervision	No Access
CEO		X
CTO	X	
CFO		X
Compliance and Legal	X	
Systems Administrator	X	
CMO		X
DPO		X
Senior Developer		X
Junior Developer		X
Support		X
Third party		X

4.6 Remote access to the system

The remote access follows the same control and procedure as the normal system access rights.

Job Description	Full Access	Read Only Access	No Access
CEO			X
CTO			X
CFO			X
Compliance and Legal			X
Systems Administrator	X		
Senior Developer		X	
Junior Developer		X	
Support	X		
DPO		X	
Third Party			X
CMO			X

4.7 Regulations for visitors

Since the production environment is being hosted by AWS, no one from the company or its visitors has access to the data centre and the physical servers.

5. Financial Accounting Procedures

5.1 Accounting Procedures

Accounting procedures are the responsibility of responsible persons of Mitrtech Operations LTD]. This responsibility may be delegated to the appropriate positions in Finance & Accounting department such as the CFO or the Head of Accounting, depending on the size of the company and internal organisational chart.

The CEO is ultimately responsible for complying with all local statutory obligations in terms of the relevant regulations within which it operates, including but not limited to the submission of statutory financial reports to respective financial authorities, tax authorities and also gaming authorities.

Accounting function may be performed in-house or may be out-sourced, depending on the extent of activities related to accounting and administration and local pricing of accounting services.

Responsible persons are also responsible for ensuring that an appropriate system of internal control is in operation to provide them with reasonable assurance that the assets of the company are being properly safeguarded and that fraud and other irregularities will be prevented or detected.

5.1.1 Chart of Accounts

Companies shall maintain chart of accounts that is compliant with local accounting standards and practices and at the same time compliant with the IFRS. At the same time the chart of accounts shall reflect the industry the company is operating and any additional internal areas of monitoring and measuring.

5.1.2 Accounting Tools

The tools used for entry of accounting data and documents need to be validated and available for common use on the market. The software is used by in-house accounting department and also external accounting service companies may have access to it.

5.1.3 Accounting Process

Main steps are the following:

- Requisition formation and approval
- Reception of documents (invoices, contracts, slips, bank statements)
- Entry of documents in accounting tool
- Archiving the documents
- Review and liquidation of documents
- Booking of documents in the accounting tool
- Payment of due amounts
- Booking of bank statements
- Reconciliation of open items.

Depending on the size of the company, some steps of the process may be joined together or organised to make the process more efficient.

5.1.4 Major Guidelines

- A Purchase cannot be made before the Requisition is approved by the responsible person;
- A document cannot be booked in the accounting tool before it is reviewed;
- A payment cannot be performed until payment package is approved by the authorised responsible person;
- Local and international Financial and Accounting Standards must be respected at all times;
- Local regulation, legislation and practice must be respected and applied at all times.

5.1.5 Cost Centres

Cost centres are intended for the management of the Company to gain additional insight of the results of areas of business the Company is in. Cost centres must reflect the nature of the industry and specifics of areas of services the Company's performing for its clients.

5.1.6 Preparation of financial statements

Financial statements shall be prepared with a frequency at least each semester of the business year. Business year applied for Mitrtech Operations LTD corresponds to the calendar year.

Financial statements shall contain balance sheet, income statement and cash flow statement for Mitrtech Operations LTD.

Deadline for preparation of financial statements is 60 days after the semester is finished.

5.1.7 Year-End Closing and Reconciliation

The Financial Accountant also reconciles all supplier statements on monthly basis.

All bank accounts are subject to written reconciliation procedures on a monthly basis with a regular independent examination of the reconciliation. All financial transactions are subject to a control account process, where all transaction balances are verified.

5.1.8 Special Gaming Reconciliation

Current and savings bank accounts are reconciled daily. All other bank and balance sheet accounts are reconciled on a monthly basis.

5.1.9 Currency

Currency used in accounting tools and for reporting in Mitrtech Operations LTD shall be Euro (EUR).

5.1.10 Archiving

The Company shall preserve and keep all financial and accounting information as required by law for at least 10 years from the end of the financial year to which it relates.

All accounting and financial records shall be kept at the company registered or operational office of Mitrtech Operations LTD.

6.2 Reporting

Reporting is done for internal and external purposes.

Internal reports are intended for the internal use of management of the Company.

External reporting is intended for any external parties that the Company interacts with. These are, but not limited to: banks, gaming authorities, central banks, statistical bureaus, potential investors, existing and potential future business partners.

6.2.1 Internal Management Reports

Internal management reports shall be prepared on a monthly basis for at least 30 days after the end of the month for which the report is prepared.

Additional internal reports shall be prepared for each semester concluded, 60 days after the end of the semester.

Reports shall include headline trading figures only, recording volumes of business and gross margin. Furthermore daily and monthly reconciliations will be carried out for all bank accounts, funds channelled through PSPs, funds held with PSPs and player deposit & Withdrawal reports.

Reports need to show actual results and comparison with prior year and budgeted figures.

6.2.2 Industry Specific Reports

Industry specific reports shall include the submission of a monthly player liability report reconciling month-end balances of all players' funds in the account's currency and in Euro, held in credit institutions in ringed-fenced accounts, and in transit, supported by credit institutions' and payment service providers' statements, with the month-end player liabilities, supported by a System report.

6.2.3 Regular Management Review

Reports shall be discussed and reviewed by the management of the Company on their monthly meetings.

6.3 Administration

The Administration is conducted at internal meetings that Mitrattech Operations LTD hosts regularly. Required attendees for these meetings are the CEO, CFO and the Key person responsible for the day to day gaming operations and the key person responsible for the administrative, financial and risk strategies. .

The administration of the Company will be effected mainly through regular management meetings attended by the Promoter (Shareholder), the Key person who is responsible for the day o day gaming operations and the key person responsible for the administrative, financial and risk strategies.

All bank accounts will be subject to written reconciliation procedures on a weekly basis with a regular independent examination of the reconciliation. All financial transactions within the general ledger will be subject to a "control account process" whereby transaction balances will be verified and reconciled on a regular basis.

Bank and e-money reconciliations will be carried out at least every two (2) working days to verify that customer deposits are being accurately reflected in the gaming system.

6.4 Reporting to the MGA/Gaming Authorities

All reports required by the MGA/Gaming Authorities will be provided by the Company's Key person responsible for the administrative, financial and risk management strategies. .

Reports on management accounts signed by the key person responsible for the administrative and financial strategies of the licensee shall be submitted for the first (6) months of their financial year, by not later than the last day of the eight (8th) month of their financial year. An audited set of financial statement shall be filed with the Authority within one hundred and eighty (180) days from the end of their financial year.

Reports provided to the MGA/Gaming Authorities shall be: monthly, interim, annual and ad-hoc reports.

6.4.1 Monthly Reports

Monthly reports show accepted bets, paid winnings, jackpot wins, jackpot funds and any pending pay-outs. Monthly reports will be submitted by no later than 20 days of the current month, for the accounting period of the previous month.

6.4.2 Interim Reports

Interim reports are prepared half-yearly and will be submitted to the MGA by latest 30 days after the period for which the reporting is made.

6.4.3 Annual Reports

Annual financial reports are prepared once a year after the last day of the year. Yearly report will be submitted to the MGA by no later than 180 days from the end of the financial year.

6.4.4 Ad-hoc Reports

Companies can also prepare ad-hoc reports. Time needed to prepare such reports may vary on the depth and complexity of the information required.

6.5 Audit

Annual financial statements of the Company are subject to be audited after they have been prepared.

External companies that will be engaged for performing audit service need to be properly licensed for performing such service and need to hold a proper reputation in the financial services industry.

6.6 Payments to MGA

The Company shall effect payment, Licensee shall effect payment to the MGA of the tax due in respect of the preceding month by not later than the twentieth day of the following month, based on the table below:

B2B Gaming Services	
Annual Licence Fee	
Where annual revenue does not exceed €5,000,000	€25,000
Where annual revenue exceeds €5,000,000 but does not exceed €10,000,000	€30,000
Where annual revenue exceeds €10,000,000	€35,000

7. Business Continuity and Disaster Recovery

7.1 Keep business recovery data and information in safe

All data and logs are stored on Amazon cloud services (AWS) and a copy of the backed-up data is stored in a different region.

7.2 Common Disruptive Events

7.2.1 Data Loss

Data is lost due to transmission or storage. This can be due to example:

- Accidentally deletion
- Malware or virus
- Hard-drive/storage breakdown
- Power failure
- Theft of servers
- Fire

A damage analysis and start of data recovery should take place immediately within 1 hour. Backups and other sources (game providers) are to be used in the recovery of data. All data should be recovered within 24 hours or a damage report should be sent to the CEO.

7.2.2 Datacentre location loss

A datacentre may be lost during a short or long period of time.

To recover from a datacentre loss, A new infrastructure will be deployed and traffic will be switched to Frankfurt region of AWS within 24 hours. All components will be moved to the DR site. The priority components are the databases and application load balancer followed by backoffice services, partner services, gameplay services, player client services, gameplay services and lastly keyops services. Once the repairs are done on the original location, traffic will be re-switched back in Ireland region of AWS

A damage report should be sent to the CEO.

7.2.3 Network loss

Due to some issues with the network to the datacentres or other connectivity, the Mitrtech services might be down. This can be due to:

- Network connectivity to game servers.
- Network connectivity to operators.
- Network connectivity to AWS (cloud service).
- Issues at the DNS server
- DDOS attack
- Error with network equipment at our datacentre location.

Any connectivity issues have attention within 1 hour. Traffic might take other routes and/or DDOS attack protection is turned on.

7.2.4 Staff loss

Loss of staff that have knowledge is one critical event. Mitrtech should always try to have staff with redundant knowledge. Within the same day, the process to find a replacement should be started and the goal is to have new staff within 3 months. Consultants could be used to temporarily fill in the knowledge gap.

7.2.5 Supplier loss

Loss of a supplier (for example bankruptcy) could have a critical impact on the services for Mitrtech. The process of replacing the supplier should start immediately.

7.3 Business Continuity Plan

The following steps are the most important:

- 1) Recover financial data, enable financial reporting and pay out to players via operators
- 2) Recover Customer data, enable facilities to resolve disputes originating from a disaster
- 3) Recover services, to resume full operations after a disaster

The time required to resume normal operations following the occurrence of each identified disruptive event shall be dependent on the nature of each disaster.

- 1) Recover financial data, enable financial reporting and payouts to players via operators – 4hours
- 2) Recover Customer data, enable facilities to resolve disputes originating from the disaster – 6 hours
- 3) Recover partner services, to resume full operations 6-24 hours

The following escalation procedure shall be implemented for each identified threat:

The Incident Response Team (IRT) is a vital part of the organisation and is responsible for handling the incidents that may occur. The IRT is responsible for taking immediate action on the incident and follow the plan defined under incident management. The team is also responsible of making sure that the set procedures are followed and improve the Incident Response Policy as well as keep it updated to the procedures and the set organisation of Mitrtech.

Each member of the IRT shall also make sure to be available for contact at all hours and for the times not being able to be in contact, provide a backup solution.

Roles and Members

Primary coordinator and point of contact:

- Markus Nasholm, Director, Mitrtech

Incident Response Team:

Markus Nasholm, Director, Mitrtech

Matias Bahlenberg, CTO, Mitrtech

Per Larsson, CCO, Mitrtech

7.4 Contact Persons

CTO, Matias Bahlenberg at matias@techasiaportal.com

Sysadmin, Anthony Lazam at anthony@techasiaportal.com

Sysadmin, Jefferson Fermo at jefferson@techasiaportal.com

Loss of staff that have knowledge is one critical event. Mitrtech should always try to have staff with redundant knowledge. Within the same day, the process to find a replacement should be started.

7.5 Test the Plan

The CTO is responsible to test the plan once a year (as minimum). The CTO should initiate a test-incident to test the current plan. It is up to the CTO to decide what kind of incident to test. A lesson learned session should take place after this test.

7.6 Alternate Sites

Company site will be recovered in a different AWS zone or region

8. Backup Procedure

The System team ensures that all backups are completed successfully and reviews the backup process on all servers daily. Logs are maintained to verify the amount of data backed-up and the unsuccessful backup occurrences. In addition, a monitoring system creates reports and raises alerts in case of backup failure.

8.1 Backup Content

Media: game images, banners and preview clip

Search: monthly based gameplay transaction indices, replicated from the database.

Database: gameplay transactions, profiles, campaigns etc.

8.2 Backup Types

Media Content will be backed up on a per version basis. The backup will be stored on S3 for 1 year.

Search content will be backed up on a daily basis. The backup will be stored on S3 for 1 year.

The Database, containing the gameplay transactions, profiles, campaigns etc. will be backed up daily, weekly and monthly. Backup data is stored in S3.

MongDB Backup Retention is as follows:

Daily snapshot is stored locally for 3 days and stored in S3 for 7 days.

Weekly snapshot is stored in S3 for 4 weeks.

Monthly snapshot is stored in S3 for 6 months.

8.3 Offsite Storage

S3 Bucket containing the blockstore is replicated on another S3 bucket residing on a different AWS region (Frankfurt) using AWS cross-region replication.

8.4 Restore Testing

Once a week the restore procedure has to run to ensure backups are restorable. This will happen in lab environment, using automated scripts. Success criteria for the test – full data consistency after restoring.

9. Document Control

Version Number	Date	Changes	Other standards affected by changes (Name standard)	Document Owner	Reviewers
1	dd/mm/yyyy	First version of the policy			
2	dd/mm/yyyy				

2018-

Markus Näshholm CEO