

Information Security Policy

Contents

1.	Our Principles	3
	Why is this important?	3
2.	Security Risk Assessment	3
	Access Controls	4
	Safeguarding of Applications	12
	<i>Antivirus/Antimalware Protection and other Perimeter Controls to Minimise Threat of Intrusion</i>	13
3.	Information Asset Management	15
	Clear Desk/Screen Policy	15
	Clear Desk Policy	15
	Clear Screen Policy	15
	Retention	15
	Backup	16
	Disposal	16
	Disposal of Media and Equipment	16
4.	Information Classification	17
	Why is it important for the Company?	17
5.	Monitoring and Compliance	18
	Security Organisation	19
6.	Exceptions	20

1. Our Principles

Why is this important?

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**.

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.

Access Controls

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.

Joiners, 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 Information Security Department.

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

¹ See “Monitoring and Compliance Section”

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 Information Security Manager.

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.

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 Gaming Authorities ("GA") (Malta Gaming Authority or Spelinspektionen), 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 Information Security Department.

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

- Minimum entry points;
- Access card;
- 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;

² See "Disposal"

- Access to the security camera equipment and footage will be restricted to authorised users;
- 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 access card/identification badge;
- 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 access cards/identification badges in a safe place when they are not within the Company Premises;
- To report lost or presumably stolen access cards/identification badges immediately in accordance with the Company's escalation procedure;
- Not to permit others, including other employees/colleagues to use their access card.

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 Information Security Department.

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 visitors 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.

Remote Access for Users

Only restricted personnel have remote access. 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).

Personnel need the authorization of Management to take their laptops out of the premises. Once authorization is granted, laptops used for remote access need to be encrypted as per Remote Access Policy. Currently, CEO, CTO and Head of Data are granted to take out their laptops out of the premises.

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 Information Security Department.

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

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.

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.

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;
- Each password must have a lifecycle of 30 days. Upon the expiry of the 30 days, the user shall be prompted to change the password. 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 15 minutes of inactivity.

Players' Password Management

Upon creating an account with the Company, players are requested to create a username and password ("login details") and provide all the relevant personal details on an online form. The account details and the access to the player's account are secured through the use of a **unique username and password**. Players are solely and exclusively responsible to keep their login details safe and secure and therefore should refrain from disclosing the same to other individuals including family members and friends. The Company confirms that players' passwords are stored in an encrypted format and are inaccessible to the Company's employees. Company employees can only access such passwords in specific circumstances which will be determined on a case by case basis and upon having obtained the approval of the Information Security Department. Players are also advised to change their passwords regularly to minimise risks.

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 Information Security 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.

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:

³ See "Remote Data Wipe"

- Approval needs to be obtained from the Information Security Department; and
- Data can only be stored in a Company provided storage device.

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 Information Security 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; and
- Adherence to the best practice security measures⁴.

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 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.

Additional Equipment Protection

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,

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

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.

Network Protection

The Company's network systems⁵ are protected by firewalls, passwords and authentication requirements, VPNs and encryption.

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 Information Security Department.

Safeguarding of Applications

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**").

⁵Also refer to Remote Access

- 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 Information Security Manager 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

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.

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 Information Security 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.

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 policy⁶ via email or otherwise, shall be encrypted.

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.

⁶ See "Information Classification"

3. Information Asset Management

Clear Desk/Screen Policy

The Company's clear desk/screen policy complements the best practice security measures mentioned above⁷.

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.

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.

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.

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.

⁷ As listed under "Device and Equipment Management"

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

Disposal

Once the retention period has expired or once it has been determined by the Company that a particular document or other material forming part of the Company Information is no longer required, it must be anonymised or securely disposed of. Paper records should be properly shredded.

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 Information Security Manager
- 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.

4. Information Classification

Why is it important for the Company?

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:

- Restricted;
- Confidential;
- Internal Use;
- Public;

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

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

Internal Use: Unauthorized access to information may cause minor damage and/or inconvenience to the organization

Public: Company Information which can be shared externally. Making the information public cannot harm the organization in any way

5. Monitoring and Compliance

The Company shall review Information Security Policies on an annual basis by carrying out an impact assessment. Assessment results shall be analysed and the Company shall develop an action plan to remedy any deficiencies within the Policy; cater for any legal or regulatory developments and changes to the business strategies.

Compliance levels will be monitored on a regular basis and results reviewed by appropriate governance bodies.

Any breach of this Policy will be treated as a serious disciplinary offence and may be subject to disciplinary actions in accordance with the provisions of the relevant Human Resources policy.

Security Organisation

CEO

The CEO shall assume the overall responsibility for compliance with this Policy

Information Security Manager

The Information Security Manager is responsible for overseeing all aspects of information security, including but not limited to:-

- Assisting the organisation in all relevant security related issues;
- Creating and distributing security policies and procedures;
- Ensuring that the relevant training and security awareness for all employees is conducted;
- Ensuring that customer demands regarding security are met and that the Company's suppliers and sub-contractors abide with this Policy;
- Undertaking overall responsibility for all Company Information processed and retained by the Company;
- Monitoring and analysing security alerts.

Department Managers

Managers of each business department are responsible for:-

- all relevant security issues concerning their area of responsibility;
- implementing this Policy within their respective departments;
- ensuring that their employees are provided with training on information security;
- monitoring their respective employees to make sure that they are fully aware and are up to date; and
- monitoring their employees to make sure they are abiding by this policy and any other associated policies especially the Incident Response Policy which describes in more detail the sequence of actions that must be taken in the event of an incident.

Users/Employees

Responsibilities include:-

- Abiding with this Policy and all relevant security policies relating to their work;
- Reporting incidents and threats to security in accordance with this Policy

Training of Employees

The Company recognises that education and raising internal awareness on the importance of information security is key. The Information Security Manager shall ensure that the training shall consist of:-

- the value of security and the importance of recognising and reporting incidents;
- the roles and responsibilities of employees in fulfilling their security responsibilities;
- understanding all the key elements of this Policy and ensuring employees are confident enough to implement them;
- basic security threats;
- the importance of compliance with legal/regulatory requirements and that misuse of computer system (including unauthorised use of information, implanting of malicious code, interference with computer systems) is a criminal offence under the Criminal Code (Chapter 9 of the Laws of Malta);
- awareness that information obtained inappropriately should not be used;
- awareness that information obtained in virtue of employment with the Company cannot be disclosed to any third party or misused, unless explicitly authorised by the Information Security Manager (in cases such as an enquiry or an investigation by a regulatory or other authority);
- awareness that breach of this policy will lead to disciplinary procedures and may give rise to a legal action against the employee.

6. Exceptions

There are no exceptions to this Policy. Any exceptions must be assessed on a case by case basis and can only be approved by the Information Security Manager.