meridian

# 1.0 Information Security Policy

## 1.1 Introduction

Information security deals with the protection of all kinds of information. It doesn't matter if the information is stored in a database, written on a post-it note or passed on in a telephone conversation. This policy protect three aspects of the information:

| **Aspect** | **Goal** | **Threat** |
|---|---|---|
| Confidentiality | Information should only be available to authorized persons. | Disclosure |
| Integrity | Information should be correct, unauthorized persons should not be able to alter the information. | Alteration |
| Availability | Information should always be available to authorized persons. | Destruction |

## 1.2 The Security Model

The purpose of the security policy is to protect valuable company assets. These assets take various forms, some are tangible and some are intangible, some are owned by the company and some are owned by a partner or a third party. The thing they all have in common is that they affect how the company conducts its business.

Throughout the security policy, the term asset shall be used to indicate any kind of asset needing protection. When a security control only applies to a particular kind of assets, the policy will clearly use a more descriptive term. Some examples of assets are:

- Data, information, back-ups, instruction manuals, user manuals
- Computers, workstations, servers, laptops, PDAs, mobile phones, media
- User applications, back office systems, accounting systems,
- Network services, the office LAN, WAN links, the Internet
- Company premises, fire alarms, air conditioners, coffee machines
- Company reputation, employee satisfaction, knowledge, experience

All assets have a designated *owner*. The owner is the person at the company who is responsible for the asset, and makes sure that the asset is working properly and that it is sufficiently protected. The owner is usually the manager at the department where the asset was created or where the asset is primarily being used. The owner has full authority over the asset and decides who should have access to it.

The daily activities of maintaining the asset is often delegated by the asset owner to a *custodian*. The custodian is only allowed to act according to the instructions from the owner. It is the responsibility of the custodian to implement the security controls specified by the security policy and the asset owner.

Everyone using an asset is called a *user* in the security policy. All employees and contractors are asset users.

The security policy sets a common standard detailing how the assets should be protected. The asset owners can set more stringent security controls on their own assets but, apart from some exceptions detailed in the policy, they cannot set lower security controls than what is specified in the security policy.

The controls included in the security policy have been selected from three different sources:

- Legal and contractual obligations, making sure the company complies with applicable law and legal agreements.
- Risk analysis, identifying the major risks to the company.
- Business security baseline, specifying a suitable minimum standard of security.

## 1.3 Format

The information security policy is divided into a set of rules. Each rule is clearly marked by using the following format:

**Rule X.Y-Z: This is a sample policy rule.**

The label Z is a numerical number providing a reference to the particular rule. When the information security policy is updated the labels will remain constant, labels are never reused. Small changes to a particular rule will not require a label change.

The label X.Y is a reference to the particular section where the rule can be found. This label might change if the rule is moved to another section or if the policy is reorganized. Therefore the X.Y label might change in the future.

The text surrounding the rules have the same normative status as the rules themselves. The text of the actual rule shall be considered a summary of the complete rule.

## 1.4 Definitions:

The following terms are used in the policy:

| | |
|---|---|
| **Business need** | Something that is needed in order to perform business. |
| **Critical system** | A system that is specified as critical in the asset inventory. |
| **Criticality** | An assets need for availability. |
| **Employee** | Throughout the security policy the term “employee” shall include contractors, i.e the term will be used to designate any person who is working for the company, unless explicitly stated otherwise. |
| **He** | For brevity, the term “he” will be used to designate an individual regardless of gender. |
| **Public services** | The Internet services that are provided by the company for public use. |
| **Security** | In the context of the security policy, the term “security” always means “information security”, i.e the protection of confidentiality, integrity and availability. |
| **Sensitive** | An asset classified as restricted or confidential. |
| **Sensitivity** | An assets need for confidentiality. |
| **Shall/should** | The word “shall” indicates a mandatory control or action. The word “should” indicates a strong recommendation. |

## 1.5 Information security policy

### *1.5.1 Security framework*

The security framework consists of the following:

- **Security statement** — The security statement is a general statement from the company board that states the needs and goals for information security.
- **Security policy** — The security policy make up the major part of the information security rule set. Complying with the security policy is mandatory.
- **External policies and procedures** — The security policy sometimes refers to external policies or procedures, these shall be considered a part of the security policy.
- **Security guidelines** — The security guidelines offer an interpretation of the security policy and gives advice on the best security practices. The security guidelines are maintained by the security group.
- **The security group** — The security group is a select group of people at the company that has been assigned the task of handling all practical security work. The group serves as a central focal point for all security issues. All questions regarding security should be directed to the security group.
- **Asset inventory** — The asset inventory holds information about all assets. The inventory is maintained by the security group but the individual asset owners are responsible for the information about their respective assets.

- **Incident management procedure** The incident management procedure is used by the security group to handle all security related incidents.

- **Risk management procedure** The risk management procedure is used as a tool for identifying the need for information security. It is used by the asset owners.

- **Business continuity plan** The business continuity plan is a document describing how to maintain business activity after major failures or disasters.

The security framework shall be reviewed every 6 months, initiated by the security group composed of the CTO and departmental managers in consultation with the asset owners and custodians. The review shall start with the risk analysis and the result from the analysis shall be used when reviewing the security policy, business impact analysis and business continuity plan.

**Rule 1.1-1: Information about all assets shall be entered into the asset inventory and be maintained by the asset owners. All changes to the asset inventory shall be logged.**

The asset inventory shall include the following:

- Name, type and location of the asset.
- Identity of the owner and custodians.
- Security classification.
- Criticality value.
- Scheduled activities.
- Information about risk analysis and review.
- Other information as identified by the security policy.

To simplify handling and reducing the number of items in the inventory, several assets can be grouped together and entered as a group into the inventory.

Only the identity of the asset, the asset owner and custodians information shall be accessible by the company employees, all other information shall be accessible only by the asset owner, custodians and the security group.

**Rule 1.1-2: Asset owners shall have security authority and responsibility for their respective assets.**

The responsibility only applies to information security. All other responsibilities, such as responsibilities originating from local legislation, is assigned by other methods.

**Rule 1.1-3: Asset owners shall mark critical assets in the inventory.**

An asset shall be considered critical if a temporary asset unavailability will affect vital business operations.

**Rule 1.1-4: Risk analysis shall be performed on all assets every 6 months by the asset owners.**

The risk analysis is initiated by the security group.

**Rule 1.1-5: Business impact analysis shall be performed every 6 months and a business continuity plan shall be developed, maintained and tested.**

The business impact analysis will identify serious threats against the business operations. The business continuity plan shall document reactive actions showing how to maintain business

activity in case of a serious disaster. The plan shall be tested as detailed as possible to make sure it is applicable in a real-life disaster situation.

Copies of the plan shall be stored in the homes of the persons involved in the plan, to make sure it is always available.

**Rule 1.1-6: Contact shall be maintained with external security specialists.**

This is to ensure that security competence is available in an emergency.

**Rule 1.1-7: User access rights shall be reviewed every 6 months by the asset owners.**

All asset owners shall do a review of the access rights to their assets.

**Rule 1.1-8: Users shall be educated about the security policy every 6 months.**

It is sufficient to keep a short refresher course and inform the users of changes to the security policy.

**Rule 1.1-9: All procedures identified in the security policy shall be documented and maintained by their owners.**

### 1.5.2 General security

**Rule 2.2-10: All users shall comply with the security policy and the documented external policies and procedures identified in the security policy. Exceptions can be made by the security group or when handling an emergency. All exceptions shall be approved in writing before considered valid.**

Complying with the security policy and the documented procedures are mandatory for all employees at all times. There are only two exceptions to this rule:

- **After approval**

  Exceptions may be granted after approval by the owners of the affected assets and the security group. Applying for such exceptions shall be in writing and specify

  - the reason for wanting an exception,
  - the involved assets,
  - an assessment of the business need,
  - an assessment of the involved risks,
  - a time limit on the exception,
  - a statement where the asset owner accepts all risks involved, and
  - the signature of the asset owner.

  Any granted exception will be valid for a maximum time period of 3 months after which it will be reviewed. If the exception is still valid at the time of a security policy review, the exception shall be considered for inclusion in the ordinary security policy.

- **Incident response actions**

  Exceptions to the security policy are temporarily granted if needed to react to a security incident, or to prevent an immediate serious security threat from being realized. No prior approval is needed in these cases. However, the security group and the owners of the affected assets must be notified immediately.

**Rule 2.2-11: Any employee violating the security policies and procedures shall be subject to disciplinary measures which might include termination of employment and criminal prosecution. Disciplinary measures shall be documented in the disciplinary procedure.**

**Rule 2.2-12: All managers are responsible for making sure that their employees are properly informed about the security policy.**

**Rule 2.2-13: All security incidents, weaknesses and security related software malfunctions shall promptly be reported to the security group. The security group shall monitor and evaluate all such events.**

**Rule 2.2-14: The security group shall supervise and audit company operations and document any deviations from the security policy. Security related issues shall be regularly reported to the company management.**

### 1.5.3 Information classification

**Rule 3.3-15: All information shall be classified by its owner. All information shall be labelled to indicate its classification.**

Some types of information is more sensitive than others. To make sure that everybody knows how to handle all kinds of information, information needs to be classified. The class of the information determines how it will be handle it. There are four classes of information:

- **Public** Public information is the kind of information that has been made public through authorized channels. It does not need any special kind of protection. Examples:
  - Press releases.
  - Public information on the web pages.

- **Internal** Internal information is information that is supposed to be known by all employees. It should be protected from outsiders, but need no special protection inside the company. Examples:
  - Information on the intranet server.
  - The internal phone book.
  - Policies and guidelines.

- **Restricted** Restricted information is the type of information the employees mostly work with and produce. This information is usually known by the employees within a single department or project, but it should be protected from other parts of the company. Most information in the company will most likely be classified as restricted. Examples:
  - Source code.
  - System documentation.
  - Marketing plans.

- **Confidential** This is the most sensitive kind of information. Disclosure of this information can cause severe damage, even if the disclosure is only internal within the company. Examples:
  - Financial information.
  - Passwords.
  - Sensitive source code.

All information shall be labelled. Labelling is needed to indicate the classification level so that others know how to handle the information. Labelling shall be done in the following ways:

| **Media** | **Labelling** |
|---|---|
| Documents | Classification is put in the header of all pages and clearly visible on the front page. |
| Text files | Classification is put in a comment line somewhere in the first few text lines. |
| Magnetic media | Classification is put on adhesive label. |
| Information on computer displays | This only applies to information generated on computer displays by applications used by the company. A default classification is specified for the software. Classification is put on all information more sensitive than the default classification. |

Other information media shall be labelled in similar ways.

**Rule 3.3-16: The security classification can only be changed by the asset owner or custodian.**

If there is a certain event or date that will trigger a reclassification, information about that event or date should be noted in the classification of the asset.

**Rule 3.3-17: Assets containing information of more than one class shall be classified to the most sensitive classification of the contained information.**

**Rule 3.3-18: When information is disclosed to a third party the information shall, where applicable, be marked as proprietary, specify the company as its owner and include a legal statement.**

### 1.5.4 Information protection

**Rule 4.4-19: Access to assets shall require a legitimate business need and only be granted after approval from the asset owner.**

When a user is given access to a particular asset the user is only allowed to use the asset for the intended purpose. The access can be restricted in different ways, e.g. an access for reading does not mean that the user may make copies of the information or alter it in any way. When in doubt the asset owner shall always be contacted.

**Rule 4.4-20: All users shall use assets only for the intended purpose and protect the assets according to the security policy and the instructions from the asset owner.**

Information shall only be handled in accordance with the following table.

| Type of information | Internal | Restricted | Confidential |
|---|---|---|---|
| Information on paper in company office | | Keep in locked compartment, must not be left on desk after regular working hours. | Keep in locked compartment, must not be left on desk when workplace is left unattended. |
| Information on paper in transit | | Do not leave unattended at any time. | Do not leave unattended at any time.<br><br>Generally not allowed, only allowed in extreme circumstances. |
| Information on whiteboards | | Must not be visible to unauthorized persons.<br><br>Information must be properly erased after whiteboard use. | Not allowed. |

| Type of information | Internal | Restricted | Confidential |
|---|---|---|---|
| Information on office workstations | | Screensaver with password required. | Screensaver with password required.<br><br>Must be encrypted. |
| Information on mobile computers | Screensaver with password required. | Screensaver with password required.<br><br>Must be encrypted. | Screensaver with password required.<br><br>Must be encrypted. |
| Information on removable media | | Must be encrypted. | Must be encrypted. |
| Information passed on during phone calls | | Other party of phone call must be identified. | Other party of phone call must be identified.<br><br>Do not use unencrypted GSM calls.<br><br>Do not use GSM phones at airports. |
| Printing information | | Care must be taken to make sure the information is sent to the correct printer.<br><br>Printouts must be retrieved immediately. | Care must be taken to make sure the information is sent to the correct printer.<br><br>The printer must be actively monitored or guarded until the printout is retrieved. |

| Type of information | Internal | Restricted | Confidential |
|---|---|---|---|
| Information sent as fax | | Generally not allowed.<br><br>Care must be taken to make sure the information is sent to the correct destination. | Generally not allowed.<br><br>Care must be taken to make sure the information is sent to the correct destination.<br><br>Reception must be verified by manual check with recipient. |
| Information passed through wireless computer networks | Must be encrypted. | Must be encrypted. | Must be encrypted. |
| Information passed through internal computer networks or internal email | | | Must be encrypted. |
| Information passed through external computer networks or external email | | Must be encrypted. | Must be encrypted. |
| Information data media in transit | Must be encrypted. | Must be encrypted. | Must be encrypted. |

Where the policy is requiring a screensaver with password, that screensaver must be configured to be automatically invoked after the computer has been idle for a maximum of 5 minutes.

Phone books, address books and calendars stored on mobile phones or PDAs are excluded from the encryption requirement.

When working in public areas such as on trains or airports, care shall be taken to protect the used equipment and keep sensitive information out of the line of sight of other people. Conversations with fellow employees shall be done in a way that sensitive information cannot be overheard.

Confidential information shall not be passed over GSM phones that don't use encryption. GSM calls can be unencrypted if the local GSM operator doesn't support encryption. Most GSM phones will indicate this fact with a warning icon in the display. However, GSM calls in Sweden are always encrypted if both the phone and SIM card were purchased in Sweden.

**Rule 4.4-21: Business information shall be stored on media that is being backed up regularly.**

**Rule 4.4-21.1: Legal documents that are not valid anymore shall be archived.**

Legal documents, include those that are not valid any more, shall never be disposed of.

**Rule 4.4-22: When information is not needed any more it shall be erased safely. Data storage media and equipment shall be safely erased before equipment is disposed of or reused.**

When information is not needed any more it shall be disposed of in a secure manner. Information on paper that is restricted or confidential shall be shredded or destroyed in a similar way. All information on data storage media and equipment, regardless of its classification, shall be given to the security group for safe destruction.

For any equipment that shall be taken offsite, the Malta Gaming Authority will be notified using adequate forms such as the Equipment Decommissioning Form. The Key Official is the responsible person to inform the MGA and submit all required documentation; furthermore he/she shall be in regular contact with the CTO and the IT Department for any changes planned/unplanned. Moreover no hard disks will be taken offsite until they are adequately destroyed, sanitized or degaussed.

**Rule 4.4-23: A client computer that has an active data connection to a remote service shall, in addition to the classification of the client computer, also be protected according to the classification of the remote service.**

**Rule 4.4-23.1: Disclosure of information shall only be done after approval by the information owner. Information regarding the financial status of the company shall only be done in accordance with the Information disclosure policy.**

## 1.5.5 Personnel security

**Rule 5.5-24: All job definitions shall specify the security roles and responsibilities.**

**Rule 5.5-25: All employees shall be screened during job application. The screening shall include check-up of references, CVs and qualifications. The identity of the employee shall be verified.**

**Rule 5.5-26: All employees shall sign a confidentiality and non-disclosure agreement.**

**Rule 5.5-27: There shall be a standardized procedure with activities to be performed when an employee is beginning or ending the employment.**

The procedures shall be used immediately when an employee is beginning or ending the employment.

**Rule 6.6-28: The physical security perimeter shall be protected and use physical entry controls.**

Company premises shall be protected from unauthorized entry by using swipe cards or other similar means that offer sufficient protection and accountability. Similar entry controls shall be used between different secured areas within the company premises.

**Rule 6.6-29: Facilities with special security requirements shall have increased protection. Special rules shall apply when working in such areas.**

**Rule 6.6-30: Physical access shall be restricted to those who have a legitimate business need.**

**Rule 6.6-31: Technical equipment shall be physically protected from environmental risks and unauthorized access.**

### 1.5.6 Communications and operations management

**Rule 7.7-32: All changes to and deployment of important server application or operating system software shall follow a standardized procedure. The procedure shall include rules for system acceptance criteria.**

The deployment procedure is a separate document that applies to the deployment of all kinds of server software in systems that are classified as important or critical.

**Rule 7.7-35: Standardized configuration templates shall be used when configuring critical server systems. Such templates shall be produced for all critical server systems and be reviewed every 6 months.**

To prevent configuration errors all relevant server systems shall be analyzed and standardized configuration templates be produced. These templates are specific for a certain server type and version, and shall specify the details of the configuration of that particular server type. Whenever a critical server system is to be configured the standardized template shall be used.

All templates shall be reviewed every 6 months to make sure they are still valid.

**Rule 7.7-36: Critical server systems shall have their configuration validated against the configuration templates. Such verifications shall be done at the time of deployment, one month after deployment and then once every third month.**

To make sure the critical servers are configured correctly the server configuration shall be validated against the configuration templates at regular intervals. The validations shall be done immediately at the time of deployment and after one month to make sure that nothing has changed during the initial server tuning and debugging. After the first two checks the validations shall be done every third month.

**Rule 7.7-37: Servers shall have their computer clocks synchronized.**

All servers shall synchronize their clocks to an accurate time source, making the clocks synchronized with an error of maximum one second. This will make it possible to trace events, compare events on different servers and use as forensic evidence in the case of criminal prosecution.

**Rule 7.7-38: Development, testing and operational systems shall be separated.**

**Rule 7.7-39: Critical assets shall be maintained in accordance with the instructions provided by the manufacturer of the hardware and software involved.**

**Rule 7.7-40: Segregation of duties shall be implemented whenever possible on sensitive systems.**

Sensitive systems need to be protected from unauthorized access. This can be achieved by implementing systems where sensitive tasks have to be done on several separate systems or by several different people. On sensitive systems this kind of segregation of duties shall be implemented whenever possible.

**Rule 7.7-41: When outsourcing a risk analysis shall be done and security controls be included in the outsourcing contract. The service provider shall inform the company of all security related incidents.**

The outsourcing contract shall include the following:

- A list of security controls.
- Specification of accepted levels of service and availability.
- Rules for compensation if accepted levels are not reached.

If possible, the company shall have the right to inspect the facilities of the service provider.

**Rule 7.7-42: Applicable security patches shall be installed promptly. System vulnerabilities shall be continuously monitored.**

Patches shall only be installed after their effect on the system has been evaluated.

**Rule 7.7-43: Resource usage of servers shall be continuously monitored and logged.**

**Rule 7.7-44: Logging of user commands shall be used on critical systems.**

**Rule 7.7-45: All computers shall be protected against malicious software, viruses and intrusion. All users shall be educated about malicious software and intrusion.**

Malicious software includes viruses, worms and trojans. All computers where malicious software is considered a threat shall be sufficiently protected by using protective software or network filtering. To prevent attacks from trojan code or similar software, all users shall be educated about these problems.

The following prevention action methods are taken against viruses and intrusion:

- Prevent unauthorized access or theft of data
- Prevent network attacks such as man-in-the-middle and probes
- Prevent software vulnerability and malicious code attacks of devices that will be used to connect to the system and application
- Prevent Denial of Service attacks
- Prevent software vulnerability and malicious code attacks of the system and applications installed

Before any deployment of new features/modules or any major change several rigorous tests are conducted to identify any weaknesses and ensure the robustness of the whole set-up.

Anti-virus software shall be deployed on all systems commonly affected by malicious software and systems facing outside environment. It is important that the most recent version of the anti-virus software and signature files shall always be installed and activated. Update interval shall be set to a maximum of 15 minutes.

The anti-virus software must check all files prior to execution. If a virus is suspected or found, it must be reported as a security incident.

Periodic scans of system shall be enabled and occur at least once per day.

Logging of anti-virus software activity shall be enabled both on client and server environment. This includes, but is not limited to, updates of software, virus definition, any suspected viruses found, and completion of periodic scan. Logs shall be retained for at least one year.

Communication solutions shall be designed so as to protect networks against interruption of service and intrusion. Documented history logs should be maintained to follow up service interruption and intrusion.

**Rule 7.7-46: Operators shall keep a manual log of operational system changes.**

The log shall be manual and include high level events such as changes to configuration or hardware.

**Rule 7.7-48: Backups of important information shall be done according to a backup and archiving policy. Backup media shall be protected from environmental risks and unauthorized access.**

**Rule 7.7-49: System logs shall be saved and archived according to the backup and archiving policy.**

All-important system logs shall be saved, archived and eventually deleted. The system owner shall specify what information shall be saved in logs and how long those log files shall be saved on archiving media.

**Rule 7.7-50: Secure Communication Protocol**

Any application or software implemented by the company shall use the Hypertext Transfer Protocol Secure (HTTPs) as a secure communication protocol for the transfer and communication of any player sensitive data, and specifically during the player registration process, the changing of password process, logon process, play, deposit and withdrawal of funds process.

### 1.5.7 Safeguarding of Applications and Networks

**Rule 8.8-50: All users shall be registered at the start of employment. The user shall be assigned a unique identifier which shall be used for access control on all assets.**

**Rule 8.8-51: Use of functional logins shall be permitted only after the user has authenticated with a personal login identifier.**

A functional login is a login identifier that is not directly connected to a particular user. To facilitate auditing and traceability, controls shall be implemented that requires a user to first login using a personal login identifier before switching to a functional login.

**Rule 8.8-52: Access shall be controlled by the owner of the accessed asset. The owner shall approve all user registrations and access changes.**

The owner always has full control over access restrictions for his assets. The practical work of configuring the asset is usually done by the custodian. It is very important that the owner gives the custodian clear instructions on the access policy.

**Rule 8.8-53: Asset owners shall document a privilege assignment policy which shall be stored in the asset inventory. The privilege assignment policy shall define a number of user types and document the privilege and access requirements of each type.**

All asset owners shall identify the types of users that need access to the asset. How the types are defined depends on the asset, a computer system might define “users” and “administrators”, while the asset owner of a company building might distinguish between users from different departments.

When the different user types are identified the asset owner needs to specify what kind of access rights shall apply to each different user type. The list of user types and their access rights shall be documented in the privilege assignment policy and be stored in the asset inventory.

**Rule 8.8-54: Asset access and privileges shall be reviewed every 6 months by the asset owner.**

**Rule 8.8-55: Asset authorizations shall be as restrictive as possible.**

**Rule 8.8-56: Login passwords and other credentials shall follow the rules outlined in the information security policy. Technical measures that enforce correct password selection shall be implemented where available.**

Passwords shall conform to the following rules:

- Shall be at least 8 characters long.
- Shall not contain part of the user's name or account name.
- Shall not include words found in a dictionary.
- Shall not be based on or similar to any previously used password.
- Shall contain characters from at least three of the following four categories:
  - English uppercase letters (A-Z)
  - English lowercase letters (a-z)
  - Numerical digits (0-9)
  - Special characters (e.g !$#%)

Passwords shall be changed at least every 90 days and not be reused.

Login accounts shall be locked after 3 consecutive authentication failures.

Wherever possible, systems shall be configured to require that the user is changing his password when he logins for the first time after the user account has been created or had the password changed by the system administrator.

**Rule 8.8-57: Passwords used for logging in to critical systems shall not be the same as passwords used for logging in to non-critical systems.**

The information security policy allows users using the same password for multiple systems. However, passwords to critical systems shall be separated from password to non-critical systems. It is still allowed to use the same password to all critical systems, as long as that password is not used on any non-critical system.

**Rule 8.8-58: Access to network services shall be controlled by the network access policy.**

The network access policy shall control all network connections, including:

- Connections from the Internet to the public services
- Connections from the Internet to the The Company office network
- Connections from the office network to the public services

- Connections from the office network to the Internet

The network policy shall regulate access to network services and specify requirements for authentication and encryption.

**Rule 8.8-59: Network connections originating from the Internet to non-public company services shall require strong encryption and strong authentication.**

**Rule 8.8-60: Back-end systems' users automatic log-off.**

Back-end systems shall automatically log-off back-end systems users after one hour of inactivity. Back-end systems users would be required to logon again in order to access back-end systems.

### 1.5.8 Cryptographic controls

**Rule 9.9-71: Selection of algorithms and key lengths shall comply with the encryption policy.**

There are many different algorithms available for encryption, decryption, signing and secure hashing of information. Several of these algorithms are available in different versions and with different sizes of the involved keys.

To make sure that the chosen implementations are safe and sufficiently strong, the security group will maintain a list of approved algorithms.

**Rule 9.9-72: Storage of Player Passwords.**

Player passwords shall be stored in the back-end system in one way cryptographic hash format and no case will be visible to back-end users.

**Rule 9.9-73: Storage of Player Payment Information**

No players' credit card number or any other player payment information will be stored in the back-end systems.

## 1.5.10 Use of company resources

**Rule 10.10-72: Company resources shall be used to perform company business. Some private use of company resources is allowed if it does not have a negative impact on business operations. No private use that might be considered as controversial is allowed. It could for example be controversial to female, masculine, political or ethical opinions.**

The company reserves the right to inspect the employee's usage of company resources at any time. The reservation includes the content on computers and mail.

**Rule 10.10-73: Company email addresses shall not be published for other purposes than conducting company business.**

Employees are not allowed to use any email address related to The Company or an The Company partner for any other purpose than conducting approved business. Publication in other contexts, e.g in phone books or on personal home pages, is not allowed.

**Rule 10.10-74: Company email addresses shall not be used when discussing in public Internet forums.**

This is to prevent business intelligence attacks using the Internet. It is very easy for a competitor to do an Internet search on the The Company domain name and find out what kind of issues the The Company employees are discussing. Use of this information can disclose details about our technical platform and business decisions.

### 1.5.11 Document management

**Rule 2.11-75: All approved business documents shall be produced and stored in accordance with the document management policy.**

The document management policy shall include rules for producing, labeling, storing and retrieving documents. The policy shall specify that the information contained in approved documents shall include the title, date, revision, security classification and the identities of the author and owner of the document.

The document management policy can define exceptions from the document management rules.

**Rule 11.11-76: Documents used internally shall be prepared in a data format that is usable on all applicable computer platforms and operating systems.**

It is important that all documents are available to all employees regardless of the kind of computer system used.

**Rule 11.11-77: Documents shall be stored in a central repository. It is the responsibility of the document owner to make sure the document is correctly stored and protected.**

Details on the document repository can be found in the document management policy.

**Rule 11.11-78: Documents being sent to external parties shall always use the Portable Document Format.**

The PDF format provides a complete and consistent visual representation of a document that can be accessed on all kinds of computers. Using this format guarantees that an external party can always read the document while at the same time making it difficult for the external party to change the information. If supported, the documents shall be locked to further prevent alteration.

It is the company's policy that no confidential, personal or operation related data to be stored and portable media devices. In cases where it is of utmost necessary to have this information stored on such devices additional security is applied using specialised software to encrypt the data on the hard disks and harden the Operating Systems.

### 1.5.12 Delegation of responsibility and authority

This section applies to all kinds of responsibility, it is not limited to responsibility for information security.

**Rule 12.12-79: Responsibility and authority shall always be delegated together.**

Responsibility shall never be delegated without also delegating the authority needed to fulfil the responsibility. Also, authority shall never be delegated without responsibility.

## 1.8 Appendix

### *1.8.1 Glossary*

| | |
|---|---|
| **Authentication** | The process of verifying the authenticity of something, usually the identity of a user. |
| **Non-repudiation** | Non-repudiation is used to provide proof that a message has been sent or received. When sending a message to someone, a signed and time stamped statement may be requested that says that the receiver has indeed received the message. This statement can then be used to prove that the transaction has taken place.<br><br>Non-repudiation is a standard service that is usually implemented by using digital signatures of message checksums. Note that the signature, along with the complete message, has to be stored and saved as proof. |
| **Strong authentication** | User authentication that is based on at least two of the following four factors:<br><br>• Something the user knows, e.g a password.<br>• Something the user has, e.g a hardware password generator or smartcard.<br>• Something the user is, this includes biometrical analysis such a fingerprint or retina scanners.<br>• Something the user does, e.g writing his signature. |

**Strong encryption**

Encryption is considered strong if the chosen algorithms and key lengths provide an adequate protection that has been thoroughly tested and is not susceptible to exhaustive key search attacks.

The security group will evaluate and provide a list of approved cryptographic algorithms and methods.

## 1.8 Asset types

The following is a non-conclusive list of asset types.

| Type | Description |
|---|---|
| Area | Physical area, such as a building, floor or room. |
| Document | |
| Human resources | |
| Legal | |
| Mobile computer | |
| Server | Computer server system. Note that the important individual services are considered as separate assets. |
| Service | A subsystem on a computer server, offering some kind of service. |
| Software in-house | |
| Software third-party | |
| Workstation | |

meridian

## Revision History

| Date of Change<br>2021.11.22. | Responsible Person<br>Boris Corni | Summary of Change | Policy Created |
|---|---|---|---|
| 2023.03.03 | **Boris Corni** | **Revision** | |