



Information Security Policy

APPROVALS

All approvals are maintained and controlled in the **[Document Control System]**

Please refer to the **[Document Control System]** for the current controlled revision and approval records.

Draft and Archived/Obsolete revisions are not to be used.

Access [Document Control System] system to verify revision.

Version Control				
Version	Date	Security Class	Responsible Person	Purpose
1	21/01/2021	Confidential	Renzo Vella	Creation of Document
1.1	22/02/2021	Confidential	Edgar Portelli	Revision of Document
1.2	14/7/2021	Confidential	Edgar Portelli	Updated 21.5.3
1.3	9/8/2021	Confidential	Edgar Portelli	Updated Point 21.4 relating to Unauthorized Access to Laptops.

Table of Contents

1.	Introduction	5
1.1.	<i>Purpose</i>	5
1.2.	<i>Scope</i>	5
1.3.	<i>Policy</i>	5
1.4.	<i>Objective</i>	6
1.5.	<i>Audience</i>	6
2.	Information Security Manager	6
2.1.	<i>Information Security Manager Responsibilities</i>	6
3.	Information Handling	7
3.1.	<i>Overview</i>	7
3.1.1.	<i>High Risk</i>	7
3.1.2.	<i>Confidential</i>	7
3.1.3.	<i>Public</i>	7
4.	Personal Responsibility	7
4.1.	<i>Overview</i>	7
4.1.1.	<i>Classification</i>	7
4.1.2.	<i>Internal Withholding of Information</i>	7
4.1.3.	<i>Irregularities</i>	8
5.	Risk Assessment	8
5.1.	<i>Overview</i>	8
5.1.1.	<i>Immediate Measures</i>	8
5.1.2.	<i>Risk Assessment Log</i>	8
6.	Data Classification Policy	8
6.1.	<i>Data Classification</i>	8
6.2.	<i>General Rules for Data Classification</i>	9
6.3.	<i>Data Classification Process</i>	9
6.4.	<i>Security Requirements for Classes of Data Classification</i>	10
6.4.1.	<i>High Risk</i>	10
6.4.2.	<i>Confidential</i>	10
6.4.3.	<i>Public</i>	10
7.	Access Control & Password Policies	11
7.1.	<i>General Principles</i>	11
8.	Virus Prevention Policy	12

9.	Intrusion Detection Policy	13
10.	Internet Security Policy	13
11.	Email Policy	13
12.	System Security Policy	14
13.	Servers & Workstations	15
14.	Asset Deployment & Maintenance	15
15.	Application Development	16
16.	Physical Security & Access Control	16
17.	Digital Security	17
17.1.1.	<i>Administration</i>	17
17.1.2.	<i>Network</i>	17
17.1.3.	<i>Access Control</i>	17
17.1.4.	<i>Workstations</i>	18
17.1.5.	<i>Backup</i>	18
17.1.6.	<i>Data Loss</i>	18
17.1.7.	<i>Security Software</i>	18
18.	Data Transfers	18
19.	Acceptable Use and Ethics	18
19.1.	<i>Overview</i>	18
20.	Physical Security	19
20.1.	<i>Overview</i>	19
20.1.1.	<i>Facility Security</i>	19
20.1.2.	<i>Printed Information Security</i>	20
20.1.3.	<i>Equipment Security</i>	20
21.	Laptop Security Policy	21
21.1.	<i>Introduction</i>	21
21.2.	<i>Physical Security Controls for Laptops</i>	22
21.3.	<i>Virus Protection of Laptops</i>	22
21.4.	<i>Controls against Unauthorized Access to Laptop Data</i>	22
21.5.	<i>Other Controls for Laptops</i>	23
21.5.1.	<i>Unauthorized Software</i>	23
21.5.2.	<i>Unlicensed Software</i>	23
21.5.3.	<i>Backups</i>	24
21.5.4.	<i>Laws, Regulations and Policies</i>	24
21.5.5.	<i>Inappropriate Materials</i>	24

22.	Destruction of Information	24
22.1.1.	<i>Decommission of Digital Information</i>	24
22.1.2.	<i>Decommission of Physical Information</i>	25
22.1.3.	<i>Decommissioning of Equipment</i>	25

1. Introduction

1.1. Purpose

The purpose of the Information Security Policy is to provide a comprehensive and detailed policy addressing the handling and protection of sensitive information, digitally and physically.

1.2. Scope

The Information Security Policy applies to all areas of operation wherever and whenever for its users.

1.3. Policy

Information must be protected from a loss of confidentiality, integrity and availability, while regulatory and legislative requirements must be met.

Business continuity plans must be produced, maintained and tested regularly.

Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

Education must be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This must be tailored to the role of the individual, network administrator, system administrator, data custodian, and users.

All breaches of information security, actual or suspected, must be reported to, and investigated by, the Information Security Manager. The appropriate incident reporting procedures must be followed.

Other guidance and procedures (such as system access control and backup procedures) within this manual support this policy.

It is the responsibility of each employee to adhere to the Information Security Policy and all employees have a responsibility to conduct themselves in an ethical manner.

Non-compliance with this Policy will be subject to Management review and action in conformance with RELIGA disciplinary procedures.

1.4. Objective

By information security we mean protection of RELIGA data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose and objective of this Information Security Policy is to protect RELIGA information assets, including data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation, from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimize business damage.

The purpose of the information security policy is:

- To establish an operation-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of RELIGA and allow the same to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.
- To make available in a secure way, all data sources on a need-to-know basis.

1.5. Audience

The Information Security Policy is intended for everyone handling or coming in contact with sensitive information. All affected personnel are obligated to ensure complete compliance with the Information Security Policy.

2. Information Security Manager

The Information Security Manager is a resource appointed to oversee the compliance and enforcement of the Information Security Policy.

The Information Security Manager must ascertain that appropriate training is provided to data owners, data custodians, network and system administrators, and users.

2.1. Information Security Manager Responsibilities

- Enforce the Information Security Policy.
- Educate, inform and train personnel.
- Develop the Information Security Policy.
- Evaluate the state of the information security.
- Responsible for information classification.
- Responsible for information security routines.

- Manage systems supporting the Information Security Policy.

3. Information Handling

3.1. Overview

RELIGA information should always be regarded as intellectual property and should always be handled as such.

Information is further classified into three (3) security classes determining its importance and sensitivity. If any uncertainty in regard to security class arise, the information should always be treated as high risk until a security class can be determined. The 3 security classes are defined as follows.

3.1.1. High Risk

Information, which if disclosed, is deemed to potentially produce grave damage or be undermining in one or more areas to RELIGA or its partners. Information concerning personal integrity and information with legislative or regulatory functions is also defined as high risk as well as information concerning intellectual property or trade secrets.

3.1.2. Confidential

Information, which if disclosed, is deemed not to expose RELIGA or its partners or result in damage. Information that is not regarded as trade secrets.

3.1.3. Public

Information that can be released publicly and passed on by third party.

4. Personal Responsibility

4.1. Overview

All personnel handling sensitive information are expected to sign and adhere to the Information Security Policy at all times.

4.1.1. Classification

All personnel are expected to be able to differentiate between security classes with high risk being the dominant one and how to handle all types of information.

4.1.2. Internal Withholding of Information

If information needs withholding from individuals or other parts of the organization, it's the author, owner or department of that information that is responsible for withholding it. The practical means of withholding information can vary. The Information Security Manager can assist in this process.

4.1.3. Irregularities

Any internal or external irregularities are to be discretely and directly reported to the Information Security Manager.

5. Risk Assessment

5.1. Overview

The state of the information security should constantly be assessed. The Information Security Manager is responsible for risk assessment together with assisting competences.

5.1.1. Immediate Measures

For risks and vulnerabilities considered critical, the Information Security Manager can order immediate proactive measures to be taken.

5.1.2. Risk Assessment Log

A risk assessment meeting should be held quarterly addressing identified potential risks, their implications and prioritization as well as recommendations to appropriate measures. This is to be recorded in the risk assessment log.

6. Data Classification Policy

6.1. Data Classification

It is essential that all data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. Three classes of data have been identified:

- High Risk - Information assets over which there are legal requirements for preventing disclosure. Data covered by local and international legislation, are in this class. Payroll, personnel, gaming, player and financial information are also in this class because of privacy requirements. This policy recognizes that other data may need to be treated as high-risk because it would cause severe damage to RELIGA if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

- Confidential - Data that would not expose RELIGA to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.
- Public - Information that may be freely disseminated.

6.2. General Rules for Data Classification

Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

No system or network subnet can have a connection to the Internet without the means to protect the information on those systems reflecting its confidentiality classification.

Data custodians are responsible for creating data repositories and data transfers which protect data in the manner appropriate to its classification.

High-risk data and confidential data must be encrypted during transmission over insecure channels.

All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed in a manner consistent with industry best practices for the security level of the data.

6.3. Data Classification Process

The process consists of the following steps:

- Information system owners review the pre-defined categories as mentioned above to locate matches for all information system data for which they are responsible.
- The detailed classification information for the particular data category is reviewed to ensure their definition of the data matches the same definition. The steps above are repeated for each identifiable type of data within the information system. If any data type within the system does not appear to fit into a pre-defined category then the IT Security Manager will work with the information system owner to complete an analysis and classification of the data.
- The data category is officially recorded for each data type processed or stored by the information system.

- When all data types constituting the information system have been classified, then the security categorization of the information system will be determined based on the most sensitive or critical information received by, processed in, stored in, and/or generated by the system under review. The Steps include the following: (i) review identified security categorizations for the aggregate of information types; (ii) determine the system security categorization by identifying each of the security objectives (confidentiality, integrity, availability) based on the aggregate of the information types; (iii) assign the overall information system impact level based on the highest impact level for the system security objectives; and (iv) document all security categorization determinations and decisions.

6.4. Security Requirements for Classes of Data Classification

6.4.1. High Risk

Irrespective of the specific security implementation determined by the data owner, high risk data shall have at a minimum the following security requirements:

- The database containing the high risk data shall be encrypted;
- Limited access in accordance with a strict need to know basis;
- Change Password requirement at least every 30 days;
- Minimum password requirements are 8 alpha numeric characters;
- System logs should be reviewed regularly;
- All connections to the Internet must go through a properly secured connection point to ensure the network is protected;
- Databases that store credit card numbers or personal information should be located on an internal network and protected by a firewall;
- No access shall be granted to high risk data from mobile computers;

6.4.2. Confidential

Such data shall have at a minimum the following security requirements:

- Limited access in accordance with a need-to-know basis and sharing of such data shall require the prior authorisation of the data owner;
- Change Password requirement at least every 60 days;
- System logs should be reviewed regularly.

6.4.3. Public

Such data shall have at a minimum the following security requirements:

- Change Password requirement at least every 90 days;
- System logs should be reviewed regularly.

7. Access Control & Password Policies

7.1. General Principles

Data must have sufficient granularity to allow the appropriate authorized access. There needs to be a balance between protecting the data and permitting access to those who need to use the data for authorized purposes.

Access to the network, and servers and systems, should be achieved by individual and unique logins, and should require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.

Users must not share user names and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. Exceptions may be allowed under specific scenarios and under specific authorization by the Information Security Manager. All users must secure their username or account, password, and system access from unauthorized use.

Users must change their password regularly and new passwords must be unique from previously used passwords.

System user accounts should regularly be reviewed and audited for malicious, obsolete, and unneeded accounts.

Inactive system accounts shall be disabled following notification from the Human Resources Department. The notification from the HR Department shall be either of the following:

- An employee has terminated his appointment or has been terminated;
- A subcontractor has terminated his relationship or his contract has been terminated;
- An employee had changed his function.

Accounts should be locked after multiple password failures.

All users of systems that contain high-risk or confidential data must have a strong password. Basics for creating a strong password include a minimum length of eight characters which should include a mix of uppercase, lowercase, punctuation, special and space characters. Empowered accounts, such as administrator, must be regularly changed.

Encrypted passwords should be enabled on any devices where it is not on by default.

Users who leave their workstations should enable a password-protected screensaver or log off to prevent unauthorized access.

Passwords must not be placed in emails unless they have been encrypted.

Default passwords on all systems must be changed after installation. All administrator accounts must be given a strong password.

Logins and passwords should not be coded into programs or queries, or stored on a database unless they are encrypted or otherwise secure.

Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination.

Transferred employee access must be reviewed and adjusted as found necessary.

Monitoring must be implemented on all systems, including the recording of logon attempts and failures, successful logons, and date and time of logon and logoff.

Activities performed as administrator or super user must be logged.

Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.

System logs should be reviewed regularly.

8. Virus Prevention Policy

The introduction of computer viruses into RELIGA environment is prohibited, and violators may be subject to prosecution.

All servers should be protected by virus prevention and detection software. The software shall be configured in a way that only the system administrator may modify the changes to the settings.

All desktop systems, servers and workstations that connect to the network must be protected with an approved, licensed antivirus software product that it is kept/automatically updated.

Virus prevention software should be configured at least with the following characteristics:

- Incoming email to be scanned;
- External media to be scanned;
- Email attachments to be scanned before opening;
- Should a virus be detected, the system shall not allow the opening or running of the file;

- Automatic updates on desktops, laptops and terminals shall be inadvertently set.

Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned.

System or network administrators should inform users when a virus has been detected.

Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Users must not tamper with or disable antivirus software installed on their workstations.

Any virus detection should be followed up in accordance with the incident response policy and procedures.

9. Intrusion Detection Policy

Intruder detection must be implemented on all servers and workstations containing data classified as high risk.

Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.

Server, firewall, and critical system logs should be reviewed frequently and alerts should be transmitted to the administrator when a serious security intrusion is detected.

Intrusion tools should be installed where appropriate and checked on a regular basis. Intrusion detection tools shall be configured in a way which will allow the system administrator to identify any attempted or successful threats. This shall be carried out in a way where the system administrator is instantly notified via email or alert.

If an intrusion is detected or suspected, the system administrator shall inform the employees and service providers of RELIGA and shall follow up in accordance with the incident response policy and procedures.

10. Internet Security Policy

All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high-risk and/or confidential.

11. Email Policy

Email equipment and messages are property of RELIGA.

Messages that are created, sent or received using RELIGA email system are the property of RELIGA.

RELIGA reserves the right to access and disclose to relevant entities the contents of all messages created, sent or received using its email system.

Users must be very careful when opening email attachments.

All email communication must be handled in the same manner as a letter, fax, memo or other business communication.

Sensitive data in the email or any attachments must not be transmitted in clear text over the Internet.

No copyrighted or proprietary information is to be distributed via RELIGA email system.

Any urgent Virus warnings should be channeled to the Information Security Manager for verification of authenticity.

Email messages should not have any content that may be considered offensive or disruptive. Offensive content includes, but is not limited to, obscene or harassing language or images, racial, ethnic and sexual or gender specific comments, or images or other comments or images that would offend someone on the basis of their religious, ethnicity or political beliefs, sexual orientation, national origin or age.

Employees may not retrieve or read email that was not sent to them unless specifically authorised by the Key Information Security or by the email recipient.

Employees may not execute attachments to emails received when these are executable files.

12. System Security Policy

All systems connected to the Internet should have a vendor-supported version of the operating system installed.

All systems connected to the Internet must be current with security patches applied.

System integrity checks of host and server systems housing high-risk data should be performed.

13. Servers & Workstations

Databases that store personal information should be located on an internal network and protected by a firewall.

Publicly accessible web servers should be located on a DMZ so they are separated from the internal network by a firewall.

Mobile computers that connect to the internet must have a personal firewall and up-to-date antivirus software installed.

Antivirus scanners should be installed on all servers and workstations and should be updated with the latest virus definitions.

All development, testing, and production systems should be updated with the latest vendor security patches.

14. Asset Deployment & Maintenance

All changes to firewalls must be reviewed and authorized by the Information Security Manager and logged for future reference.

Changes to the production environment should be authorized and logged before being implemented.

When an employee leaves RELIGA, that employee's corporate user accounts and passwords should be immediately revoked.

Remote maintenance accounts should be enabled when needed and disabled when the maintenance process is complete.

All access to sensitive data should be logged.

Successful and unsuccessful login attempts and the accessing of the audit logs should be logged.

System clocks should be synchronized, and log files should contain date and time stamps.

The firewall, router, wireless access points, and authentication server logs should be regularly reviewed for unauthorized traffic.

Audit logs should be regularly backed up, secured, and retained for at least three months online and one year offline for all critical systems.

Vulnerability scans or penetration tests should be performed on all applications and systems before they are put into a production environment.

All internet points of presence should be scanned daily using services which provides intrusion detection and prevention functionality.

Before going into production, all devices must undergo a lockdown procedure where unnecessary or default services, protocols, settings, accounts, and passwords are changed or disabled.

Only secure, encrypted communications should be used for remote administration of production devices.

15. Application Development

Software and application development should follow industry best practices and include information security throughout the development life cycle.

Web application should be designed using accepted security guidelines.

Web application authentication processes should not reveal if usernames or passwords are correct - only that a login failed or was successful.

User information that is stored in cookies should be encrypted.

All web application input validation should be performed by the server, not by the client.

The minimum information to be required upon authentication should be a unique username and password.

16. Physical Security & Access Control

Multiple physical security controls should be implemented to prevent unauthorized access to data centres.

Equipment and media containing sensitive information should be physically protected from unauthorized access.

The distribution and disposal of backups and other media containing sensitive information should be handled in accordance with a procedure approved by the Information Security Officer.

Media that contains sensitive information should be inventoried and securely stored.

Media that contains sensitive information should be deleted, shredded, or degaussed before disposal.

17. Digital Security

17.1. Overview

Digital security covers the software security measures in place to prevent unauthorized access, data loss and manipulation.

17.1.1. Administration

Software systems in use should have sufficient security built in to support the Information Security Policy. The Information Security Manager evaluates software and systems to ensure compliance. The Information Security Manager oversees the IT administrators managing software and systems in use.

17.1.2. Network

The network infrastructure should be designed to support the Information Security Policy and only be accessible by authorized personnel. Any wireless networks should be sufficiently secure. Connections to the internet should be secured and protected.

17.1.3. Access Control

The Information Security Manager establishes account types or user group definitions and their associated permissions. IT administrators manage software access control locally under the supervision of the Information Security Manager.

17.1.3.1. Accounts

Accounts should be distributed and managed by IT administrators. Accounts or usernames contains a personal name or equivalent identification with a set of associated user rights or user groups attached to it.

17.1.3.2. Means of Authentication

Means of authentication are distributed and managed by IT administrators. The means of authentication must comply with the Information Security Policy and only allow access to authorized personnel.

Passwords are required to strictly follow recommended security models and expire within recommended time cycles.

17.1.4. Workstations

Workstation software should be operated by authorized personnel only. Only users and administrators should be able to operate workstation software.

17.1.5. Backup

In house developed content should be versioned and backed up to remote locations at all times. Operational and released software should be backed up redundantly in accordance with the local legislations and regulations. *For backup information see Data Backup Procedure.*

17.1.6. Data Loss

If data is lost due to human factor or malfunction, the incident is to be reported to the Information Security Manager.

17.1.7. Security Software

Security software should be used to prevent and detect intrusions and unwanted software. IT administrators should manage the security software.

18. Data Transfers

Data containing sensitive information should only be transmitted through secure and encrypted channels if possible.

Communication services should be evaluated by the Information Security Manager who gives recommendations to administrators and users.

Email should be filtered and scanned by security software for unwanted content.

Personal or private data transfers should not be permitted.

19. Acceptable Use and Ethics

19.1. Overview

Users of software systems are trusted to abide to the acceptable uses and ethics defined as follows.

- Users may install software trusted by the IT administrators or the Information Security Manager.
- Computer systems should always be used with the Information Security Policy in mind.
- Users should regard all aspects of a computer system as RELIGA property and accept inspections and monitoring by IT administrators without prior notice.
- Users should not install license requiring software without obtaining a valid license first.
- Users should not use computer systems for personal or private profit.
- Users should not engage in any illegal or immoral activity whilst utilizing RELIGA computer systems or equipment.

20. Physical Security

20.1. Overview

Physical security covers the physical security measures in place to prevent and restrict unauthorized personnel from accessing, stealing or manipulating sensitive information and securing information in the event of an emergency.

20.1.1. Facility Security

All local facilities that handle sensitive information should have a set of security measures in place.

20.1.1.1. Safes

Safes should be used to store High Risk information in digital or printed form. Safes should be fireproof to ensure information is secured in the event of a fire. Access to safes should be managed by the Information Security Manager.

20.1.1.2. Emergency Routines

There should be emergency routines in place for every facility. Personnel should be educated and informed about such routines.

20.1.1.3. Physical Security Providers

Physical security providers should install alarms, educate personnel and handle physical access to the facility. The physical security providers should also provide monitoring and on site security in the event of a security breach. The responsibility of the security of facilities is shared between security providers and Office Assistants.

20.1.2. Printed Information Security

Documents containing high risk information should be stored in safes or archives when not in use. When in use, the documents should be kept in close proximity at all times and only handled by authorized personnel. If a document is found missing the incident is to be reported to the Information Security Manager.

Documents containing confidential information should be stored in archives when not in use. When in use, the documents should be kept within sight and handled by authorized personnel. Third parties can view confidential documents as seen fit.

Documents containing public information should be stored as seen fit and can be viewed by anyone.

20.1.3. Equipment Security

Equipment security covers all hardware security aspects. The Information Security Manager with assistance from administrative personnel evaluates and recommends hardware. All hardware used must be fully capable of complying with the Information Security Policy.

20.1.3.1. Inspections

All local equipment should be subject to inspection to ensure no hardware is altered or not used in accordance with the Information Security Policy.

20.1.3.2. Network Equipment

All network equipment should be located within a secured facility, numbered and kept in records.

20.1.3.3. Portable Media

Portable media should be located within a secured facility or in close proximity to authorized personnel. Portable media should be numbered and kept in records. Private portable media should not be allowed within facilities.

20.1.3.4. Workstations

Workstations should be located within a secured facility. Workstations should be numbered and kept in records. Workstations should be closed entities without easy access to internal parts.

20.1.3.5. Servers

Servers should be located within a secured facility. Servers should be numbered and kept in records. Servers should be closed entities without easy access to internal parts.

20.1.3.6. Mobile Devices

Mobile devices should be located within a secured facility or in close proximity to authorized personnel. Mobile devices should be numbered and kept in records. Private mobile devices should be highly restricted. Mobile devices should be stored in safes or security lockers when not in use.

20.1.3.7. Service Providers and Remote Sites

Certified service providers are to be trusted to manage physical security for all facilities and equipment containing sensitive information.

20.1.3.8. Loss of Equipment

If equipment containing sensitive information is lost or not accounted for, the incident is to be reported to the Information Security Manager. If information storing equipment fails or is damaged it must be subject to destruction and not repair.

21. Laptop Security Policy

21.1. Introduction

This policy describes the controls necessary to minimize information security risks affecting RELIGA laptops.

All RELIGA computer systems face information security risks. Laptop computers are an essential business tool but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside RELIGA premises increases the threats.

Portable computers are especially vulnerable to physical damage or loss, and theft, either for resale or for the information they contain.

The impacts of such breaches include not just the replacement value of the hardware, but also the value of any RELIGA data on them, or accessible through them. Information is a vital RELIGA asset. We depend very heavily on our computer systems to provide complete and accurate business information when and where we need it. The impacts of unauthorized access to, or modification of, important and/or sensitive RELIGA data can far outweigh the cost of the equipment itself.

This policy refers to certain other/general information security policies, but the specific information given here is directly relevant to laptops and, in case of conflict, takes precedence over other policies.

21.2. Physical Security Controls for Laptops

The physical security of any laptop is one's personal responsibility so all reasonable precautions should be taken.

Laptops should be retained in the possession of the owner's sight whenever possible, especially in public places.

Laptops should be locked away out of sight when they are not in use, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel.

Laptops should be carried and stored in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage.

Note should be taken of the make, model, serial number and the RELIGA asset label of any laptop.

21.3. Virus Protection of Laptops

Viruses are a major threat to RELIGA and laptops are particularly vulnerable if their antivirus software is not kept up-to-date. The antivirus software MUST be updated at least monthly. The easiest way of doing this is simply to log on to the RELIGA network for the automatic update process to run.

Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.

Any files should be virus-scanned before they are downloaded to any laptop computer from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically.

Any security incidents (such as virus infections) are to be reported promptly to the IT Department in order to minimise the damage.

Virus warning message on your computer, or if there is any suspicion of a virus infection (e.g. by unusual file activity), are to be responded to immediately by the IT Department .

Special care should be taken to virus-scan any system before any files are sent outside RELIGA. This includes email attachments and CD-ROMs that you create.

21.4. Controls against Unauthorized Access to Laptop Data

All laptops need to be joined to the company's internal domain.

Access to the laptops is controlled through the Active Directory and not using the local laptop users.

All active Directory users that will be accessing the laptop, need to be part of the Default Account and Password Policy within the Active Directory.

The Account and Password Policy needs to have the below configuration:

- Enforce password history – 24 passwords remembered
- Maximum password age – 42 days
- Minimum password age – 2 days
- Minimum password length – 10 characters
- Password must meet complexity requirements – Enabled
- Account lockout duration – 30 minutes
- Account lockout threshold – 5 invalid attempts

The holder of the laptop is personally accountable to store their data on the Company's Network Drives and not locally on the laptop.

All Laptops have the 'Malware Bytes Add-on' installed and enabled, for Real-Time Malware and Virus Threat detections.

The holder of the laptop is personally accountable for all network and systems access under his/her user ID, so passwords shall be kept secret. Passwords should not be shared with anyone, not even family members, friends, or IT staff.

Corporate laptops are provided for official use by authorized employees. Laptops should not be loaned or allowed to be used by others such as family and friends.

Laptop should not be left unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

21.5. Other Controls for Laptops

21.5.1. Unauthorized Software

No-one should download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into RELIGA networks, as well as affecting the working of your laptop. Software packages that permit the computer to be 'remote controlled' (e.g. PCAnywhere) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly forbidden on RELIGA equipment unless they have been explicitly pre-authorized by management for legitimate business purposes.

21.5.2. Unlicensed Software

Extra care should be taken about software licences. Most software, unless it is specifically identified as “freeware” or “public domain software”, may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and RELIGA into disrepute by breaking the law.

21.5.3. Backups

Local Data is not backed up. Only Files saved on the Network Drives are Backed up Automatically.

21.5.4. Laws, Regulations and Policies

Relevant laws, regulations and policies applying to the use of computers and information are to be complied with. Software licensing has already been mentioned and privacy laws are another example. Various corporate security policies apply to laptops, the data they contain, and network access (including use of the Internet). Visit Information Security’s Intranet website for further information.

21.5.5. Inappropriate Materials

RELIGA will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites. IT staff routinely monitor the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If you receive inappropriate material by email or other means, delete it immediately. If you accidentally browse an offensive website, click ‘back’ or close the window straight away. If you routinely receive a lot of spam, call the IT Department to check your spam settings.

22. Destruction of Information

22.1. Overview

The Information Security Manager is responsible for all activities concerning destruction of company information. The Information Security Manager signs agreements with certified IT disposal providers when needed and oversees signoffs.

22.1.1. Decommission of Digital Information

Digital information destined for decommission should be logged ensuring records of all destroyed equipment is kept. Hard-drives and flash memory is erased and media shredded before signoff to IT disposal provider.

Information contained in remote location or in connection with online services should be removed to the best extent possible.

Information residing in rented equipment is erased at the end of contract periods before control is returned to the service provider.

22.1.2. Decommission of Physical Information

Printed information is logged and recorded and shredded if possible before signoff to IT disposal provider.

22.1.3. Decommissioning of Equipment

The decommissioning of any equipment from the data centre should be carried out only by the persons who are authorized to enter the data centre.

All decommissioning of equipment is to be notified to the Key Information Security and the Key Information Security will via the prescribed Decommissioned Equipment form notify the Malta Gaming Authority (the “**Authority**”).

Should prior notification not be possible the decommissioning equipment form should be submitted within 24 hours of the decommissioning.