

SOFTRIOS N.V.
Registration number: 172758

Information Security Policy

Revision History:

Date	Description	New Version
05 December, 2025	First Version	1.0

Contents

1	Corporate Information Security Policy Statement	6
1.1	Objective	6
1.2	Scope	6
1.3	Policy Statement	6
1.4	Responsibilities	6
1.5	Enforcement	7
1.6	Standard	7
1.7	Compliance	7
2	Acceptable Use Policy	7
2.1	Introduction	7
2.2	Purpose	8
2.3	Scope	8
2.4	Policy	8
2.4.1	General Use and Ownership	8
2.4.2	Security and Proprietary Information	8
2.4.3	Unacceptable Use	9
2.4.4	System and Network Activities	10
2.5	Compliance	11
2.6	References	11
3	Email Policy	11
3.1	Purpose	11
3.2	Ownership	11
3.3	Usage Policy	11
3.3.1	Non-Business Email	12
3.4	Compliance	12
4	Internet Security & Usage Policy	12
4.1	Purpose	12
4.2	Ownership	13
4.3	Usage Policy	13
4.3.1	Non-Business Browsing	13
4.4	Compliance	13
5	User Management Policy and Standards	13

Information Security Policy

5.1	Objectives	13
5.2	Scope	14
5.3	Policy.....	14
5.3.1	Control of Entry to a System	14
5.3.1.1	Identification	14
5.3.1.2	Authentication	14
5.3.1.3	Authorisation	14
5.3.2	Terminating User Access.....	15
5.3.3	Miscellaneous Access Controls	15
5.3.3.1	Dormant and Dead Accounts	15
5.3.3.2	Automatic Lockout (Screenlock)	15
5.3.3.3	Unsuccessful Login Attempts	15
5.4	Compliance	16
6	Anti-Virus Policy.....	16
6.1	Introduction	16
6.2	Policy.....	16
7	Password Policy & Standards.....	16
7.1	Purpose.....	16
7.2	Scope	16
7.3	Ownership.....	17
7.4	Policy.....	17
7.4.1	Password Administration	17
7.4.2	Composition	17
7.4.3	Responsibilities & Maintenance.....	17
7.4.4	Important Passwords	18
7.5	Monitoring	18
7.6	System Security.....	18
8	Media & Equipment Disposal Policy	18
8.1	Disposal of Media	18
8.2	Disposal of Equipment	19
9	Data Ownership and Classification Policy	19
9.1	Purpose.....	19
9.2	Policy.....	19
9.2.1	Responsibilities	19
9.2.1.1	Data Owners	19

Information Security Policy

9.2.1.2	Data Custodians/Processors.....	19
9.2.1.3	Data Users.....	19
9.2.1.4	Management.....	19
9.2.2	Assigning Ownership.....	19
9.3	Data Classification Standards.....	20
9.3.1	Data Classification Standard	20
9.4	Data Protection Measures	20
10	Laptops and Portable Devices.....	21
10.1	Introduction	21
10.2	Policy.....	21
11	Intrusion Prevention Policy	21
11	Intrusion Prevention Policy.....	21

1 Corporate Information Security Policy Statement

1.1 Objective

Information Security is a principal asset of SOFTRIOS N.V. ("the Company") and as such appropriate measures must be employed to protect this valuable asset and ensure against its unauthorised modification, disclosure or destruction.

1.2 Scope

This policy applies to all information in the company's possession, whether held on computer systems or otherwise. The policy is applicable to all personnel employed or working with the Company, regardless of their position, location or relationship with the Company.

1.3 Policy Statement

It is the Company's policy to ensure that:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity and availability of information will be maintained;
- Regulatory and legislative requirements will be met;
- Continuity plans will be produced, tested and maintained;
- Information security awareness amongst all staff will be created through the provision of regular training sessions;
- All breaches of information security, actual or suspected, will be reported to, and investigated by the person or persons responsible for security;
- Copyright of intellectual property will be respected; and
- Information will be protected against malicious code.

1.4 Responsibilities

The Key Person has direct responsibility for maintaining the policy and providing advice on information security and guidance on its implementation. The policy will be reviewed and maintained annually, or in case of any changes in the applicable legislation.

The Management is responsible for implementing this policy within their business area and for ensuring that all employees understand their obligations to protect the Company's assets and comply with security standards and related procedures.

- All employees have a responsibility to conduct themselves in an ethical manner.
- Data/information obtained inappropriately should not be used.
- Finding a system weakness is not a license to take advantage of it.
- Every user has a responsibility to carry out his/her work diligently and will be held accountable for misuse of the Company's computer systems.

Information Security Policy

- When the confidentiality of information is unclear, its classification should be ascertained.
- Report any known violation or system weakness to the person or persons responsible for the Company's security or to your line manager.
- All intrusions should be reported, investigated and the Incident Response Policy should be adhered to.

1.5 Enforcement

Non-compliance with this Policy will be subject to Management review and action in conformance with the Company's disciplinary procedures.

1.6 Standard

Other related policies, all supporting standards, procedures, guidelines, operating instructions issued in support of this policy statement, will form an integral part of this Information Security Policy and shall serve as a standard to be applied by the Management. It can also serve as a basis of compliance monitoring and review.

1.7 Compliance

All information held or processed by the Company that is not publicly available should be kept internal and undisclosed. Consequently, any breach of secrecy is a definite breach of the Company's policy. The use of electronic communications and computer systems is subject to the provisions on unauthorised access, interference and damage to automated systems, as set out in Articles 2:69 to 2:70, 2:73 to 2:74 and 2:107 to 2:108 of the Criminal Code of Curaçao (Wetboek van Strafrecht Curaçao). The protection and processing of personal data are governed by the *National Ordinance on the Protection of Personal Data (Landsverordening bescherming persoonsgegevens A.B. 2010 No. 84)*, which entered into force on 1 October 2013. In addition, the European Union *General Data Protection Regulation* (GDPR) may apply extraterritorially where the processing of personal data concerns individuals located within the European Union. This policy is designed to guide employees in ensuring compliance with all relevant legal requirements concerning information security and data protection.

2 Acceptable Use Policy

2.1 Introduction

The company's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Company's established culture of openness, trust and integrity. Management is committed to protecting the company's employees, partners, Account Holders and the company itself from illegal or damaging actions by individuals carried out either knowingly or unknowingly.

Internet/Intranet-related systems, including but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, and any documentation are the property of the Company. These systems are to be used for business purposes in serving the Company's interests, and those of our clients and customers in the course of normal operations.

2.2 Purpose

The purpose of this policy is to outline the general acceptable use of computer equipment and documentation in our company. These rules are in place to protect the employees, the Account Holders and the Company. Inappropriate usage will expose the Company to risks such as virus attacks, compromise of network systems and services, and legal issues. Other policies specific to areas of concern, such as email and internet usage, have been drawn up and should be consulted for more details.

2.3 Scope

This policy applies to employees, contractors, consultants, part-timers, and other workers at the Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company, the services that run on it and any documentation relevant to the equipment, products, services, clients, partnerships and the Company's business.

2.4 Policy

2.4.1 General Use and Ownership

- While the Company's IT Support desire is to provide a reasonable level of privacy, users should understand that the data they create on Company's systems remain the property of the Company. Due to the need to protect the Company's network, management cannot guarantee the confidentiality of employees' information stored on any network device belonging to the Company.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use of the Company's systems. Other policies, namely internet and email usage policy, should serve as a more detailed guide on personal use of the Company's systems, and if there is any uncertainty, employees should consult their direct superior.
- Management recommends that any information that users consider sensitive or vulnerable be encrypted or at a minimum should be password-protected.
- For security and network maintenance purposes, authorized individuals within the Company may monitor equipment, systems and network traffic at any time.
- The Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- Any documentation, inclusive of reports, is also the property of the Company and should be handled appropriately.

2.4.2 Security and Proprietary Information

- Information contained on Internet/Intranet/Extranet-related systems should be classified, as specified from time to time by the Management. Examples of confidential information include but are not limited to: the Company's corporate strategies, competitor-sensitive information, trade secrets, specifications.

- credit card data, customers' lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 20 minutes or less or by logging-off when the host PC/laptop/workstation will be unattended.
- Use encryption of information when a password is not deemed sufficient protection for the data. Secure encryption algorithms should be used, and proper key management procedures are to be followed, where applicable.
- Reports and documents containing sensitive or confidential information should not be left on desks or in areas accessible to unauthorized users. Employees must lock away any such documentation when they are not directly in control of it. At the end of the day all other documents should be cleared off the desks and stored away appropriately.
- Since information saved on portable computers is very vulnerable, it is essential that one holds only certain data that serves a business need. If portable computers are used, these data must be kept only for a particular intended period. If one holds confidential data, such data ought to be securely encrypted.
- Postings by employees from the Company's email addresses to newsgroups should contain disclaimers stating that the opinions expressed are strictly their own and not those of the Company, unless posting is in the course of their business duties.
- All hosts used by an employee that are connected to the Company Internet/Intranet/Extranet, whether owned by the employee or the Company, shall be continually executing approved virus-scanning software with an updated virus database, unless overridden by departmental or group policy.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, as these may contain viruses, e-mail bombs, or Trojan horse code.

2.4.3 Unacceptable Use

The following activities are generally prohibited. Employees may be exempted from these restrictions in the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances are employees of the Company authorized to engage in any activity that is illegal under local or international laws while utilizing Company-owned resources.

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

2.4.4 System and Network Activities

The following activities are **strictly prohibited**, with no exceptions:

- Violations of the rights of any person or companies protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Company or authorized for use by the Company.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Company or the end user does not have an active license.
- Exporting software, technical information, encryption software or technology in violation of international export control laws is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- The transfer of sensitive data between office equipment and home equipment is prohibited without management authorization.
- Using Company computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile-workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from a Company account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior approval is obtained from management.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Purposely circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial-of-service attack).

Information Security Policy

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, the Company's employees or Account Holders to parties outside of the Company.

2.5 Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2.6 References

- Criminal Code of Curaçao (Wetboek van Strafrecht Curaçao) – Articles 2:69 to 2:70, 2:73 to 2:74 and 2:107 to 2:108 (unauthorised access, interference and damage to automated systems).
- National Ordinance on the Protection of Personal Data (Landsverordening bescherming persoonsgegevens, A.B. 2010 No. 84; in force since 1 October 2013)
- National Ordinance on Electronic Commerce (Landsverordening elektronische handel, Curaçao, Publicatieblad 2013 No. 17).
- European Union General Data Protection Regulation (GDPR).

3 Email Policy

3.1 Purpose

- The sole purpose of an email is to conduct the Company's day-to-day business.
- This document outlines the Company's policy on employee responsibilities for electronic mail (email) messages sent or received via the Company's email systems. It covers internal and external network systems and services to which the Company may subscribe.

3.2 Ownership

- Email equipment and messages are the property of the Company.
- Messages that are created, sent or received using the Company's email system are the property of Company.
- The Company reserves the right to access and disclose to relevant entities the contents of all messages created, sent or received using its email system.

3.3 Usage Policy:

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

Information Security Policy

- Sensitive data in the email or any attachments must not be transmitted to clients or colleagues, in clear text over the Internet.
- No copyrighted or proprietary information is to be distributed via the Company's email system unless a Director, Key Person or Manager has granted approval.
- No commercial messages, employee solicitations, messages of a religious or political nature are to be distributed using the Company's email.
- Bulk forwarding of jokes, chain letters and other similar materials should not be effected, especially to recipients outside of the office.
- Any urgent Virus warnings should be channelled to IT sections or Key Person for verification of authenticity, as a number of such warnings are usually hoaxes.
- Email messages may not contain content that may be considered offensive or disruptive. Offensive content includes, but is not limited to, obscene or harassing language or images, racial, ethnic, sexual or gender specific comments or images or other comments or images that would offend someone on the basis of their religious or political beliefs, sexual orientation, racial origin or age.
- Employees may not retrieve or read email that was not sent to them unless specifically authorised by Company or by the email recipient.
- Employees **may not** execute attachments to emails received when these are executable files, such as, *.exe, *.vbs, *.com, .swf, irrespective of the source of the email.

3.3.1 Non-Business Email

- Incidental and occasional personal use of electronic mail is permitted. Such messages become the property of the Company and are subject to the same conditions as any other business email.

3.4 Compliance

- Violation of this policy will result in disciplinary action up and including termination of employment and/or legal action if warranted.
- Employees should report any misuse of the Company's email system or violations of this policy to the appropriate official. The identity of the staff member reporting such misuse will be treated with the strictest confidence at all times.
- Computer misuse is a criminal act and employees should be aware of the consequences.

4 Internet Security & Usage Policy

This document outlines the Company's policy on employee responsibilities for Internet usage over the Company's network.

4.1 Purpose

- The purpose of providing employees with access to the Internet is to conduct the required day-to-day business of the Company.

4.2 Ownership

- The computers and all network components are the property of the Company.
- The software installed on the computers is the property of the Company.
- Any data saved on the computers, devices, media or network is the property of the Company.
- The Company reserves the right to carry out checks on the computers, network devices and any audit logs to ensure that they are being used properly when accessing the internet. Other types
- of computer usage are covered by other policies.

4.3 Usage Policy

- All employees who require access to Internet services must do so by using the Company's approved software and Internet gateways.
- Access to illicit sites, hackers' sites or sites of a dubious nature is strictly prohibited.
- Downloading of any software or executable files is strictly prohibited.
- Internet users are reminded that Web browsers leave a trail of all sites visited.
- Technicians who need access to certain sites of a dubious nature to monitor for security holes or system vulnerabilities or other security related exercises must obtain specific permission to do so. Such access will be carried out from systems that do not contain sensitive data and the technician must at all times exert the utmost caution.

4.3.1 Non-Business Browsing

- Any such browsing can take place during breaks; however, the usage rules above will still be applicable.

4.4 Compliance

- Violations of this policy will result in disciplinary action, any measures up to and including termination of employment and/or legal action if warranted.
- Employees noticing any violations of this policy are to report them immediately to the person responsible for Information Security. The identity of any employee reporting a violation will be kept confidential at all times.

5 User Management Policy and Standards

5.1 Objectives

User Management control is to be introduced into the Company system to achieve two controls:

- a) preventing intruders from entering the system; and,
- b) limiting authorised users to their legitimate purposes.

5.2 Scope

This policy applies to all employees, contractors, Account Holders and any other party requiring access to Company data or systems wherever they are located or whatever form or shape they may take.

5.3 Policy

5.3.1 Control of Entry to a System

This will be achieved by requiring the would-be user to log on to the system by entering a User ID or User Name recognisable by the system and then a password or passphrase to confirm that he/she is the legitimate owner of the User ID. Users should not be allowed to communicate with the system in any way before completing log-on.

5.3.1.1 Identification

A User ID most often consists of a non-secret string of characters and is normally the first thing the user provides the system when attempting to "log on", i.e. to gain access.

For accountability purposes, credentials are not to be shared between individuals, neither during a user's duration with the company nor thereafter.

No one should be granted a User ID for any Company system unless that person has a recognised need to use the system and has been properly identified and authorised.

5.3.1.2 Authentication

Before being allowed to log on to a system and gain access to any resources, the user's identity must be authenticated to prevent impersonation. Whilst passwords will be acceptable on internal networks, these may not suffice for high-risk environments.

5.3.1.3 Authorisation

A user or process must be granted the right to access a system. Users with the higher levels of privilege may themselves grant access rights to resources under their control to other users or processes. In all cases, the concept of least privilege or 'need-to-know' must be adhered to.

Access rights to data files are to be decided strictly on the basis of the content and the role of the user. In addition, restricting access to other resources, such as terminals, printers, and network services, must also be considered. In particular, it is valuable to restrict the use of system administrator, security administrator, database administrator, and similar commands to a limited number of users and terminals.

The following steps must be taken before authorisation to access any resource is granted:

- Establish exactly what resources each person or group of people needs to access and in what way (eg. READ, WRITE, etc., for files), taking note of anticipated future needs;

Information Security Policy

- Standardize user identifiers and task names: the standardized names should preferably reflect the section of Company for which the data owner works;
- Define file and other resource naming standards based on the process involved, or the department/unit, or an individual.

5.3.2 Terminating User Access

Once an employee's employment is terminated, the Director must:

- Ensure that the employee's account has been closed/disabled. Where platforms are involved, the respective platform should be notified if applicable.
- keep all correspondence on file, for reference.

5.3.3 Miscellaneous Access Controls

5.3.3.1 Dormant and Dead Accounts

Dead or inappropriately privileged accounts should not be left on a system because they could provide the vehicle for misuse. Steps to take should include some or all of these controls:

- removal of vendor's accounts used for setting up the system, or changing their passwords, as the initial passwords are widely known;
- introduction of procedures to allow users to request their access rights be revoked for set periods and subsequently restored (to cater for leave etc.);

5.3.3.2 Automatic Lockout (Screenlock)

- The automatic disablement of logged-on workstations after a period of inactivity of 20 mins shall be implemented either through group policy or by the employees themselves. This feature must be implemented on laptops (if applicable).
- As well as the above automatic procedure, the user should be able to manually invoke the screenlock program.

5.3.3.3 Unsuccessful Login Attempts

- The logon procedure should throw out or lock out a person who has input an incorrect password after a pre-determined number of times.
- The number of attempts permissible before logout should be between 3 to 6 depending on the risk rating of the system or information being accessed.
- The user should not be enabled unless properly authenticated. Automatic re-enabling after a predetermined period of time should not be permitted.

5.4 Compliance

- Violation of this policy should be avoided. If deviations are absolutely necessary, then top management authority must be obtained, and documentation kept of the rationale behind the authorisation to deviate.
- Employees should report any misuse or abuse of authorisation levels or user accounts or any cases of suspected unauthorised access.
- Should an employee have access to resources and is aware that he/she should not have access to such resources, he/she should report it and refrain from using these access rights. Failure to do so will be treated as a violation of this policy.

6 Anti-Virus Policy

6.1 Introduction

The term 'anti-virus software' refers to software which scans and removes malware which includes viruses, Trojans, worms, spyware and adware.

6.2 Policy

- All equipment (servers and PCs) should have anti-virus software installed whenever available/applicable.
- Virus definition file should be automatically updated daily.
- Anti-virus software should be set to carry out periodic scans.
- Where a PC/server cannot be updated from the internet, the virus definition file should be downloaded to another machine and manually installed on the respective PC/server.

7 Password Policy & Standards

7.1 Purpose

- Passwords are used to authenticate users requiring access to a system and therefore have to be constructed and maintained in a secure way at all times.

7.2 Scope

- Users include employees and customers of the Company as well as all management and contractors, auditors, and third parties provided with access to the systems.

7.3 Ownership

- Each user on the system should have a password and that password is the property of that user only and no other person must use that password to access a system. The user is responsible for choosing a password that is difficult to guess and that complies with this policy.
- Administrators and Application Owners should ensure that adequate password standards are supported by applications and/or systems implemented.

7.4 Policy

7.4.1 Password Administration

- As each password belongs to the individual user and that password is the key to access the systems, the users therefore, have a responsibility towards the employer by ensuring that the composition and maintenance of their password conforms to this policy. In this way it will be harder for would-be wrongdoers to compromise the organisation's systems.

7.4.2 Composition

- Minimum Length of a password must be at least 8 (eight) characters for normal users and 10 (ten) characters for superusers, such as administrators, and users with access to sensitive data such as payroll.
- The password must contain characters from at least three of uppercase, lowercase, numbers and special characters.
- Select passwords that are easy for a user to remember.
- Under no circumstance must one use dictionary words, telephone numbers, family member names, number plates, easy words with numbers, one's User ID as it is or in any other form, any repeated letters or numbers.

7.4.3 Responsibilities & Maintenance

- Passwords should be changed at least every 60 days on high-risk systems, and between 120 days to 180 days on lower-risk systems. Where in doubt, one should consult the owner/s of the system and data or the IT Support.
- Passwords should not be reused until at least 4 password changes have been carried out.
- Passwords must not be written down anywhere.
- If a password is assigned to the user, the user should change it immediately to his/her own personalised password.
- Never give one's password to anyone or accept a password from anyone, especially over the phone or the Internet.

7.4.4 Important Passwords

- IT Support possesses several passwords in order to access and administer the different components/systems, such as firewall, application, back-up utility, email server, web server. The composition of these passwords is of the utmost importance and should be taken very seriously.
- Without access to this password, continuity of operations may be hampered or seriously hindered. Therefore, all owners of these passwords have to write them down on a memo and seal them in an envelope. The envelope must be signed at all ends, and then sealed with tape and placed in a safe under the control of a member of management. These envelopes should only be opened in cases where no other option or solution is available. A history of the passwords should also be maintained so that in the case of system restoration, after an emergency, the system may be accessed.

7.5 Monitoring

- Employees of the Company or consultants may, from time to time, be authorised by management to attempt to crack passwords being utilised on the Company's systems by employees. Common cracking tools will be used. Any weak passwords that are discovered will be disclosed only to the employee involved who will also be asked to change it immediately and to avoid using weak passwords.

7.6 System Security

- Any system in production should preferably be able to automatically enforce the above mentioned password policies, as this will reduce the chances of insecure passwords being used. Therefore, all systems in use that support some or all of the policies in this document should have those features enabled. All efforts should be made to develop or purchase software supporting this policy, where this is cost-effective.

8 Media & Equipment Disposal Policy

8.1 Disposal of Media

The company and its employees will comply with the following policy:

- Shred any media, such as paper, CDs, DVDs which have elapsed their retention period.
- Any Hard Discs, USB Sticks, External Hard Discs containing Company data, which no longer need to be kept on file, will be wiped-off using a secure wiping program.
- If Data Tapes are used, these will be wiped with "full erase" command via the backup software.

8.2 Disposal of Equipment

If any equipment needs to be removed from the Company's network, the Company will ensure that the Hard Disks of such equipment have been completely degaussed.

9 Data Ownership and Classification Policy

9.1 Purpose

Data is one of the Company's most valuable assets and requires responsible and ethical use. It is essential that the Company's data are classified so that security measures can be correctly implemented. It is also necessary to assign responsibilities to the handling of all data held so that security measures may be implemented and monitored.

9.2 Policy

9.2.1 Responsibilities

9.2.1.1 Data Owners

Owners are responsible for knowing, understanding and classifying all data they own. They are also responsible for ensuring that adequate security is applied to the data in accordance with the classification assigned by them and that the security satisfies all legal requirements. Only they may authorise persons to access the data and they decide the access rights to be assigned.

9.2.1.2 Data Custodians/Processors

Custodians are responsible for data entrusted to them for periods of time irrespective of the format. They are responsible for ensuring that the level of security required to protect the data is maintained during their custodianship. Examples of custodians would be IT Support.

9.2.1.3 Data Users

Users have been granted access rights to the data by the owners so that they may carry out their duties and responsibilities. Users may not abuse the rights given to them and may only do what they have been authorised to do by the owners.

9.2.1.4 Management

The owners of data and the custodians are to be appointed by the management after an understanding of the data and the roles of individuals have been achieved.

9.2.2 Assigning Ownership

The overall ownership of the data rests with the company. However, the responsibility and authority over that data will be delegated to the required Company departments and/or authorities as

Information Security Policy

deemed necessary. In doing so, however, it is recognised that ownership responsibility is not a single all-or-nothing dictatorial concept; but rather it is comprised of a set of responsibilities.

9.3 Data Classification Standards

This policy outlines the extent to which the data classification standard should be followed, the responsibilities of the departments' employees under the standard, and provides guidelines for classifying the data.

9.3.1 Data Classification Standard

Five levels of data classification have been established.

1. Unclassified/Public Domain - data that does not fall into any of the other data classifications noted below. This data may be made generally available without specific Data Owner's approval;
2. Operational Use Only - data whose loss, corruption or unauthorised disclosure would not necessarily result in any business, financial or legal loss, but is made available to Data Owner-approved users only;
3. Private - data whose disclosure would not result in any business, financial or legal loss but involves issues of personal credibility, reputation, or other issues of personal privacy;
4. Confidential - data whose loss, corruption or unauthorised disclosure would tend to damage the business, image, reputation or research capabilities of the Company, or result in business, financial, or legal loss;
5. Top Secret - data whose loss, corruption or unauthorised disclosure would be a violation of laws and regulations.

All data regardless of medium and/or form will be identified as to its classification (i.e. Unclassified, Operational Use Only, Private, Confidential or Top Secret).

Aggregates of data should be classified based upon the most secure classification level; in other words, when data of mixed classification exist in the same file, report or memorandum, the classification of the same file, report or memorandum should be of the highest level of classification.

9.4 Data Protection Measures

1. Public Domain data requires no specific protection either during storage or transmission.
2. The availability and integrity of Operational Data must be protected during transmission and storage. Systems housing and carrying such data must be securely configured and message authentication utilised during transmission. Adequate back-ups of such data must be regularly taken and stored both on-site and off-site.
3. Private data must be afforded the same level of control as operational data. In addition, should such data travel over a public network, it must do so in encrypted format to preserve confidentiality.

Information Security Policy

4. Access to Confidential data must at all times be strictly on a need to know/least privilege basis. Such data must always be transmitted in encrypted format.
5. Top Secret data must be afforded the highest levels of control at all times. Encryption during storage and transmission using the strongest techniques available. Furthermore, networks or databases housing such information should be segregated from other networks.

10 Laptops and Portable Devices

10.1 Introduction

Laptop computers (and other mobile devices) 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 utilised away from the company premises increases the threats from malicious third parties.

10.2 Policy

- Avoid leaving your laptop unattended and logged-on. Always log off or lock it before walking away from the laptop. For mobile phones, use the 'password lock' feature at all times.
- Lock the laptop away out of sight when not using it. Never leave a laptop visibly unattended in a vehicle. If necessary, lock it out of sight in the car's boot but it is generally much safer to carry it with you.
- Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage.
- Keep your mobile device within sight whenever possible. Be extra careful in public places, such as airports, railway stations or restaurants. Never leave your mobile device unattended.
- Use encryption whenever possible. If your laptop is lost or stolen, encryption provides a good protection against unauthorised access to data.
- When using laptops and other mobile devices, backups are normally the users' responsibility. Backups should be done weekly by uploading data to the company network, or if not possible by copying data to DVD/USB devices. Encrypt backups wherever possible.
- Do not share company laptops or devices with other third parties, such as family and friends.
- If your device is lost or stolen, report to your superior and to the administrator immediately.

11 Intrusion Prevention Policy

Information Security Policy

Although the operation of the Company is a small one, it is still dependent on the availability of the technical infrastructure. Intrusions of the system of the Company may be in the form of physical unauthorised access, as well as logical unauthorised access. The physical side is being addressed by the choice of the data centre for the colocation of live production equipment. The data centre abides to strict policies and procedures for the well-keeping of the equipment of its clients. Only authorised personnel can avail themselves of the access to the equipment of the Company.

Anything connected to the internet poses a risk of being attacked and getting compromised. For this reason, the network of the Company (albeit a simple one) was designed in such a way as to have both a public interface so that the web server can be reached from the internet, as well as a private network which makes it inaccessible from internet. The web server is connected to the DMZ segment whilst the database is connected to the private LAN segment. This makes it very difficult for intruders from the internet to access the database. The two servers communicate between each other via the firewall rules.

The policy adopted by the Company is one that spans over the hardware and software of the gaming system, as well as the software on the machines which connect remotely to the gaming system.

The Company will:

- Configure the firewall so that only the ports, services and internet traffic relative and necessary for the proper operation of the Company are permitted;
- Allow only encrypted connections to the production equipment;
- Use strong passwords to connect to the production equipment;
- Harden the operating system and software of the Web / Application server by applying patches and software security updates in a timely manner;
- Harden the operating system and software of the Database server by applying patches and software security updates in a timely manner; and
- Use antivirus software and update its virus definitions on a regular basis. This will be done on both the production equipment as well on the machines that remotely connect to the live equipment.
- Follow change management procedures for every change to the production environment.
- Use a reputable data centre for the co-location of the Company's equipment.