

COMPANY INFORMATION SECURITY POLICY

TABLE OF CONTENTS

COMPANY INFORMATION SECURITY POLICY	1
1.INFORMATION SECURITY POLICY OBJECTIVES	3
2.HUMAN RESOURCE SECURITY POLICY	4
2.1 PRIOR TO EMPLOYMENT	4
2.2 DURING EMPLOYMENT	4
2.3 TERMINATION OF EMPLOYMENT	4
3.ASSET MANAGEMENT POLICY	5
3.1 ASSETS AND DATA CLASSIFICATION	5
3.3 OWNERSHIP OF INFORMATION ASSETS	5
3.4 ACCEPTABLE USE OF ASSETS	6
3.4.1 EMAIL USAGE:	6
3.4.2 POLICY PERTAINING TO COMPUTER USAGE	10
3.5 INFORMATION STORAGE AND RETENTION	14
3.6 INFORMATION DISPOSAL	15
4.ACCESS CONTROL POLICY	16
4.1 ACCESS TO NETWORKS AND NETWORK SERVICES	16
4.2 USER ACCESS MANAGEMENT	17
4.3 USER REGISTRATION AND DE-REGISTRATION	17
5.CRYPTOGRAPHY POLICY	18
5.1 CRYPTOGRAPHIC CONTROLS	18
6.PHYSICAL AND ENVIRONMENTAL SECURITY	19
6.1 SECURITY PERIMETERS CONTROLS	19
7.OPERATIONS SECURITY POLICY	20
7.1 OPERATION SECURITY CONTROLS	20
7.2 PROTECTION FROM MALWARE	20
7.3 VIRUS PROTECTION	20
7.4 BACKUPS	21
8.COMMUNICATION SECURITY POLICY	24
8.1 NETWORK CONTROLS	24
8.2 SEGREGATION IN NETWORKS	24

8.3 NETWORK DOCUMENTATION.....	25
8.4 MOBILE DEVICES AND TELEWORKING	26
9.SYSTEM ACQUISITION, DEVELOPMENT AND MAINTANANCE POLICY	28
9.1 SYSTEM DEVELOPMENT CYCLE	28
9.2 PROTECTION OF APPLICATION SERVICES TRANSACTION	29
9.3 SYSTEM CHANGE CONTROL PROCEDURES	30
9.4 OUTSOURCED DEVELOPMENT	30
9.5 SYSTEM SECURITY TESTING AND ACCEPTANCE TESTING	31
9.6 PROTECTION OF TEST DATA.....	31
10.INFORMATION SECURITY INCIDENT MANAGEMENT POLICY	32
10.1 POLICY STATEMENT	32
11.INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT POLICY	33
12.DOCUMENT REVIEW	33
13.DOCUMENT APPROVAL	33

1. INFORMATION SECURITY POLICY OBJECTIVES

i. PURPOSE

The purpose of this document is to bring clarity to what our company intend to achieve through implementing this Information security Policy document. It shall stand as the security policy of our organisation.

ii. OBJECTIVES

The information security policy is established to ensure the following objectives are met.

OBJECTIVE CLASS	PARAMETER OBJECTIVE	TARGET	RESPONSIBLE PERSON
Integrity	To ensure there is no data integrity violations per year.	Zero Integrity violations	IT Manager who will delegate from time to time
Confidentiality	To ensure there is no confidentiality violation of information per year.	Zero Confidentiality violations	IT Manager who will delegate from time to time
Availability	To ensure all information resources are available all the time.	98% Availability	IT Manager who will delegate from time to time

iii. SCOPE

This policy document applies to all our company employees, contractors and premises and shall be followed all the time. It borrows concepts and best practices from GDPR.

This policy document is read in conjunction with our service provider's policies, where applicable and on request.

2.HUMAN RESOURCE SECURITY POLICY

PURPOSE

This policy has been established to adequately address the requirements of Information Security in recruitment and employment activities. Human resources department and information security officer shall be responsible for scheduling information security awareness training programs.

2.1 PRIOR TO EMPLOYMENT

There shall be:

- Independent verification of identity by means of a photographic ID such as passport or national ID.
- Confirmation of claimed academic and professional qualifications by contact with the certification authority.
- Availability of satisfactory character references, including at least one professional or business reference.
- Criminal history check.
- Credit rating / debt check.

2.2 DURING EMPLOYMENT

- All Employees and Contractors must be required to sign a confidentiality or non-disclosure agreement.
- There shall be information security awareness training for all employees.
- There shall be a formal disciplinary process to handle violations of confidentiality, Integrity, and availability of information resources.
- Awareness of this policy shall be communicated to all employees.

2.3 TERMINATION OF EMPLOYMENT

- An exit interview shall be done for those employees leaving the organisation.
- Employees leaving the organisation shall be informed of confidentiality requirements that exist even after leaving the organisation.

3.ASSET MANAGEMENT POLICY

PURPOSE

This policy has been established to provide for identification of information assets and handling of the information assets. All Our information assets are tracked and maintained in accordance with their sensitivity and criticality. Such information assets include laptops, desktops, switches, routers, firewalls, human resource, applications, databases, and any other gadget that stores or processes company information. This policy is read in conjunction with data protection policy DPP1-22.

3.1 ASSETS AND DATA CLASSIFICATION

- The organisation shall maintain up-to-date information assets register.
- The information assets shall be classified as either Public, Internal, Restricted or Confidential
- Public assets have public disclosure and their disclosure to public does not affect the organisation's information security objectives.
- Internally classified information assets must never be disclosed to the public but can be freely circulated within the organisation.
- Restricted information assets are shared between concerned members only for example employment contracts, medical files, backups storage etc.
- Confidential information assets are highly restricted and can only be shared with specifically vetted and authorised employees for example encryption keys, sensitive financial reports etc.
- Company data and information systems shall not be installed or setup on personal devices.

3.3 OWNERSHIP OF INFORMATION ASSETS

- Every Information Asset should be assigned an Asset Owner as soon as it is created or acquired.
- Asset owners are responsible for the proper management of an asset over the whole asset lifecycle.
- Asset Owners must ensure that all Information Assets are inventoried, appropriately Classified, and protected, and properly handled throughout their life cycle including during deletion or destruction.

3.4 ACCEPTABLE USE OF ASSETS

3.4.1 EMAIL USAGE:

GENERAL RESTRICTIONS:

- The Company e-mail system may not be used:
 - To initiate or forward any chain-message or other message which asks the recipient to forward such message to multiple other Users unless required for work purposes.
 - To send frequent and/or numerous e-mail messages with the intention of disrupting or inconveniencing the receiver.

RESTRICTIONS ON CERTAIN PERSONAL USE:

- The Company's e-mail system may not be used for the personal dissemination or storage of personal advertisements, solicitations, promotions, destructive programs, political material, or any prohibited material.

RESTRICTIONS ON FORWARDING MESSAGES IN CERTAIN CIRCUMSTANCES:

- The forwarding of e-mail messages without a legitimate business purpose, which is likely to lead to the embarrassment of the original sender, or in violation of the clearly expressed intention or request of the original sender to restrict further dissemination is prohibited.

PROHIBITED MATERIAL:

- The use of the Company's e-mail system to send, download, display or store prohibited materials prohibited.
- No employee shall knowingly send or store e-mail or any form of electronic communication containing prohibited material.
- If any User is uncertain as to whether any material or statement constitutes prohibited material, such User must obtain clarification from their immediate reporting line and/or the IT Manager of the Company without delay.
- E-mail containing prohibited material which has been inadvertently received by a User shall be deleted as soon as he or she becomes aware of the content thereof and the incident reported to the employee's immediate reporting line and/or the IT Manager of the Company without delay.

USERS MAY NOT DISGUISE THEIR IDENTITY:

- Users may not disguise their identity while using the Company's e-mail system.

USERS MAY NOT ALTER INDICATION OF ORIGIN:

- Users may not alter the 'From' line or any other indication of the origin of an e-mail message.

USER OBLIGATIONS ABOUT E-MAIL:**USE OF THE DISCLAIMER:**

The disclaimer will be automatically displayed on e-mail messages transmitted for and on behalf of the Company. Users shall ensure the following:

- Every e-mail message which is transmitted for and on behalf of the Company contains the Disclaimer at the start/end of every such message.
- To indicate the privacy of any e-mail communication, the User shall designate any such communication as "private" and store it in a folder identified as such.

FORMAL CORRESPONDENCE AND OTHER DOCUMENTS:

- Any formal document of the Company, which any User wishes to transmit via email, shall be sent as an attachment to an e-mail message, on the Company letterhead template provided for this purpose or other formal correspondence material.
- Users are alerted to the fact that e-mail communications can in fact bind the Company to an agreement, and as such the Users need to comply with the relevant statutory requirements and Company policies as communicated to them in this regard. If the User is in any doubt, clarification should be obtained from their immediate reporting line and/or the IT Manager of the Company; and
- All e-mail communications are the Company's records. The Company reserves the right in its discretion to access and disclose all legitimate business communications sent using the Company's e-mail system.

MISS-ADDRESSED E-MAIL:

Miss-addressed e-mail that may have been received and opened inadvertently must be deleted from the Company computer system immediately by the User receiving and opening such an e-mail. If its location on the Company computer system is uncertain, the assistance of the IT department should be sought. The User concerned should also notify the sender of such e-mail, of the circumstances of receipt of the fact that it has been deleted.

WORK RESPONSIBILITIES:

- If an employee has received an e-mail or Fax that employee is obliged to action and respond to the e-mail or Fax within a reasonable turnaround time.
- Employees who are found to delete or ignore e-mails or Faxes without auctioning, the employee will be dealt with in accordance with the Company Disciplinary Code in terms of negligence of duties.
- Should an e-mail or Fax be sent to an individual and this does not fall within the ambit of their duties, it is that specific individual's responsibility to pass the information on to the relevant manager in the department who will be able to action it.

TRANSMISSION OF COMPANY INFORMATION BY MEANS OF E-MAIL:

Users to respect the Company's proprietary material:

- Users of the Company e-mail system shall respect the Company's proprietary interest in Its confidential material.

TRANSMISSION OF CONFIDENTIAL MATERIAL:

Confidential material shall not be sent, transmitted, or otherwise disseminated by Users to third parties unless the User has satisfied himself/herself that:

- He/she is duly authorized to send, transmit or otherwise disseminate the relevant confidential material.
- It Is In the ordinary course of the business of the Company or in the Company's best Interests to send, transmit or otherwise disseminate such confidential material; and that
- Such confidential material Is already in the public domain; or
- The intended recipient is entitled to receive such confidential information or material.

RETENTION OF DATA INCLUDING E-MAIL:

- In the same way as printed documents, correspondence and material is subject to retention policies, so is the data and e-mail belonging to the Company.
- Users are required to ensure that all data that may be required to be retained by legislation or in terms of the Company's document retention policies as communicated to them, are retained, and stored in compliance with such legislation or such policies.
- If a User Is uncertain as to how to effect the retention of any data he or she shall refer to and obtain instructions from the IT department.

CONFIDENTIAL

DISCLOSURE OF DATA CONTAINED IN E-MAIL:

No User shall on his or her own accord, under any circumstances, respond in any way to a discovery notice or demand to disclose any particulars regarding the Company, e-mail or to any subpoena to produce an e-mail at any court proceedings (other than to acknowledge receipt thereof if necessary) without first obtaining the authority and advice of the Chief Executive Officer or someone authorized by him or her in writing.

3.4.2 POLICY PERTAINING TO COMPUTER USAGE

- Users are responsible for ensuring the security, integrity and confidentiality of all data and information resident on the local memory of their personal computers. In addition to the rules relating to passwords, Users shall take reasonable steps to ensure that no confidential material resident in the memory of their personal computers is:
 - i. Visible during their absence from their personal computer; or
 - ii. Otherwise, accessible by unauthorized persons.

Reasonable steps include the following:

- Enabling the password faculty on the approved screensaver program.
- Enable where applicable, a BIOS password on laptop computers, if authorized by the IT Department.
- Enabling passwords to secure the files containing confidential information; and
- To the extent possible, not storing confidential material on laptop and desktop computers amongst others.
- Saving and removing data:
 - i. Users are strictly prohibited from saving Company confidential Information data or files onto their portable computers, disc, CD-ROM, memory stick or any electronic or other storage media and removing it from the Company premises other than in accordance with this clause.
 - ii. Any User requiring access to Company confidential information, data, or files, whilst in any location other than at the Company premises, shall obtain the express permission of the Chief Executive Officer and will be subject to, inter alia, the following conditions:

- iii. The remote use of Company confidential information, data or files may only be made by Users in the performance of their work functions for and on behalf of the Company.
- iv. The Company confidential information, data or files will always remain the property of the Company and Users will not acquire any right in or assert any lien against it.
- v. The User further undertakes to protect and safeguard the confidential information, data, or files in a diligent and conscientious manner, and to perform a comprehensive virus scan where the data or information has been used on a personal computer or other device not belonging to the company, prior to re-introducing data or information onto a company computer system.
- vi. The user will promptly return the company confidential information, data or files at the request of the company and/or destroy any copies therefore and:
- vii. This clause shall not limit any other right of the company regarding its confidential information, data, or files.

All forms of tape media (including hard disk drives) must be destroyed or deleted by a process that ensures that data cannot be recovered at the end of the process whenever:

- The information is no longer required.
- The media is transferred to another User who does not have the authority to view the data; or
- The User leaves the company's employment.

User must store all corporate files on the file server (network) in the directory structure provided. IT is responsible for backing up all file servers. Although responsibility for this data resides with the Users, the responsibility for the backup of such data resides with the IT department. Users should seek the assistance of qualified IT support personnel if they are unsure whether they are adequately securing their data for back up.

Personal files should be kept on workstations and may not be stored on the fileserver, unless authorized by the IT department. Ownership of these files resides with the User, and the IT department is NOT responsible for the backing up of such data. Users should maintain backups of their data on external media where possible; and

Any failure to adhere to the provisions of this clause may not only result in disciplinary action pursuant to the provisions of this policy but may also result In the User becoming personally liable to the Company for any loss suffered because of his/her conduct.

COMPUTER SYSTEM MAINTENANCE:

The IT department is responsible to carry out any maintenance and support of the Company computer system and peripherals. Accordingly, Users may under no circumstances:

- Attempt to repair their own personal computers, or those of other Users; or
- Allow unauthorized technicians to perform any support, repair, or maintenance on the Company computer system.

Any failure to adhere to the provisions of this clause may not only result in disciplinary action pursuant to the provisions of this policy but may result in the User becoming personally liable to the Company for any damage or loss suffered by the Company because of his/her conduct.

Users must report all IT related requests for service to the IT Helpdesk, who will prioritize the call based upon its importance and allocate the necessary tasks to an appropriate person. Examples of such requests for service include:

- Suspected virus activity.
- Theft of computer equipment.
- Non-availability of network resources; and
- Password resets.

SOFTWARE USAGE:

The Company has licensed or developed certain software for use on the Company computer system. This software is proprietary to the Company and third parties. To protect its proprietary interests and to ensure compliance with the terms of applicable licenses, Users are expressly prohibited from:

- Copying Company software for use on any computer other than the Company's supplied personal computer without the written permission of the IT Manager of the Company.
- Copying or granting access to Company software for distribution to independent contractor, clients or any third party.
- Installing or downloading any software other than Company software onto the Company's computer system.

- Modifying, revising, or adopting any Computer software.
- Translating, reverse engineering or disassembling of any software resident on the Company's computer system: and
- Creating and installing software on the Company's computer system without the prior written permission of the Company.

If at any stage a User believes that a particular software product, whether freeware, shareware, or proprietary software, would assist in the furtherance of the Company's business then a motivation should be sent to the IT Department and the Chief Executive Officer of the Company.

INTERNET USAGE:

Users are prohibited from publishing or transmitting Company data of a confidential nature on or via the Internet. If a situation exists where prohibited material must be transmitted, written authorization will be required from the Company, prior to the transmission or publication of such information on or via the Internet if such authorization is conditional, all conditions shall be met before transmitting the confidential material.

Users are reminded that the Company permits predetermined number of Internet hours usage per month. The User is cautioned that prolonged Internet usage beyond the maximum during working hours may result in a full site report being published on each site visited for the month and reviewed by IT staff and Management.

The User may then be required to provide written justification to the Chief Executive Officer regarding the excessive usage. The Company will permit Internet usage above the predetermined maximum, on the condition that the usage is business related and is required to assist them in the performance of their work function. The employee's direct reporting line must approve this usage in writing.

- Users may not knowingly introduce viruses into the Company computer system; and
 - Users are prohibited from accessing websites, which contain prohibited material.
- Without derogating from this statement, the Company may apply the use of filters in respect of certain websites, which it deems to be undesirable.

3.5 INFORMATION STORAGE AND RETENTION

Asset retention period is determined in this order: Requirements of the law, whether the information is still required and below guidelines.

Document Information Type /	Classification	Storage Location	Retention Period
Financial Records, Budgets, Audit Reports.	Confidential	Accounts Filing, Computer Databases, Secured Workstations	Six years
Published marketing material, Websites.	Public	Points of distribution, marketing archive	Copies to be kept in the Company's archive indefinitely as historic record of organisation timeline and evolution.
Policies, processes, procedures, and related registers, standards.	Internal Use	Limited and controlled physical copies, general consumption through Shares with restriction on editing, downloading, and printing.	Out of date material to be removed from circulation immediately. Company Archive to hold one copy of every prior version for last 5 years.
Division and Departmental meeting minutes.	Internal Use	Shares with restrictions on editing, downloading, and printing.	Three years
Employee contracts, other HR records relating to employment lifecycle.	Restricted	Locked HR Filing Cabinet. Secured HR Workstations	Duration of employment plus four years.
Payroll information.	Restricted	Secured Payroll Server and Locked Filing Cabinets	Three years
System audit trails and log files.	Restricted	Central repository	Two years
Key Encrypting Keys.	Confidential	Dual control safe custody	Four years
PII Encryption Keys.	Confidential	Dual control safe custody	Every two years or as permitted by software
TLS and SSH Keys.	Confidential	Dual control safe custody	Every twelve months

3.6 INFORMATION DISPOSAL

Asset disposal requirements are determined by the data inside the asset.

Information / Media Type	Classification	Disposal / Destruction Rules
Paper or other hard copy	Restricted	Supervised crosscut shredding
Hard Disk and other Electronic Media	Restricted	Supervised degaussing, intense sanitisation, or incineration.
Paper or other hard copy	Confidential	Supervised crosscut shredding
Hard Disk and other Electronic Media	Confidential	Supervised degaussing, intense sanitisation, or incineration.
Paper or other hard copy	Internal Use	Shredding
Hard Disk and other Electronic Media	Internal Use	Degaussing, intense sanitisation, or incineration.

4.ACCESS CONTROL POLICY

PURPOSE

This policy has been established to ensure that all access to our organisational Information and Information Systems is formally authorised and documented while providing User accountability and ensuring all access is dependent on “need to know” and delivered on a least privilege basis.

4.1 ACCESS TO NETWORKS AND NETWORK SERVICES

- Access to Our network and systems will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- Where remote access to the network is implemented remote access policy and home working/mobile working procedures will apply.
- Privileged Access must only be provided on a need-to-use basis for the minimum requirements of a User’s functional role.
- The staff member’s line manager must approve the application.
- Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.
- Security privileges (i.e., 'super user' or network administrator rights) to the network will be allocated on the requirements of the user's job, rather than on a status basis.
- All users to the network will have their own individual user identification and password.
- Users are responsible for ensuring their password is kept secret.
- User access rights will be immediately removed or reviewed for those users who have left the organisation or changed jobs.

4.2 USER ACCESS MANAGEMENT

A formal User registration, de-registration, and provisioning process to enable the assignment of access permissions and rights must always exist. All user and system accounts must:

- Permit a maximum of three consecutive log-in failures before locking out
- Require that when an account has become locked out it remains locked out for 30 minutes or until a System Administrator unlocks it
- Provide logging of all successful and unsuccessful login attempts
- Provide a session time-out if idle for more than 10 minutes after which an account is disconnected or logged-out and then requires re-authentication

4.3 USER REGISTRATION AND DE-REGISTRATION

- Assign all Users a unique ID before allowing them to access system components or cardholder data ensuring that redundant User IDs are never assigned to new Users.
- Ensure generic User IDs are disabled or removed from all systems and devices.
- Never use shared User IDs for system administration and other critical functions.
- Remove or disable User accounts which have been inactive for 90 days.
- The Human Resources Department is responsible for issuing de-registration instructions on retirement, retrenchment, termination, or death of Employees.

5. CRYPTOGRAPHY POLICY

PURPOSE

This policy has been established to ensure proper and effective use of Cryptography to protect the confidentiality, authenticity and integrity of our organisational Information and Information related services.

5.1 CRYPTOGRAPHIC CONTROLS

Our organisation employs cryptography in numerous cases, including:

- Securing of application-level connections such as ssh, https, and RDP.
- Securing sensitive information held in databases using encryption.
- Securing Restricted or Classified information used on mobile computing devices, including on the disk drives of notebook computers.
- securing all other client – server channels such as ssh, ftps, and sstp using TLS1.2 and private keys of 2048bits length.
- securing all Restricted information held in databases or file shares using TLS1.2 and private keys of 2048bits length.
- Ensuring that all secrets, symmetric keys, and private keys used for encrypting links, services or data are backed-up and stored securely.
- Encryption keys must never be shared between production and test systems. Test systems must use different keys to their associated production system.
- Encryption keys must be served in key vault to ensure their security.
- Data at rest and data in transit shall be encrypted to ensure its integrity and confidentiality.
- Data under processing shall be protected through implementation of clean desk policy.

6. PHYSICAL AND ENVIRONMENTAL SECURITY

PURPOSE

This policy has been established to prevent unauthorised physical access, damage and interference to our organisational Information Assets and Information Processing Facilities.

6.1 SECURITY PERIMETERS CONTROLS

- Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. IT manager will maintain and periodically review a list of those with unsupervised access to critical network equipment.
- Network computer equipment will be housed in a controlled and secure environment.
- Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
- Surveillance camera is installed to monitor and record footage.
- Critical or sensitive network equipment will be protected from power supply failures using Uninterruptible Power Supply (UPS) devices.
- Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.
- Smoking, eating, and drinking is forbidden in areas housing critical or sensitive network equipment.
- Entrance to organisational premises shall be controlled by use of access tags
- Closed circuit television shall be installed to monitored physical security environment.

7. OPERATIONS SECURITY POLICY

PURPOSES

This policy has been established to provide for the correct and secure operation of our Information Processing Facilities by protecting them from malware, hardening technical vulnerabilities, recording, and storing log files, and maintaining appropriate operating procedures, change management, and Information backups.

7.1 OPERATION SECURITY CONTROLS

- Procedures for the operation of Information processing facilities must be documented and available to those who need them.
- All system changes must be approved before implementation and must be documented.
- Implementation of security software and patches must be done.
- All configuration or system changes must be planned before implementation.
- Development/Testing and production environments must be completely separated from each other.

7.2 PROTECTION FROM MALWARE

- Preventive, detective, and recovery controls against malware must be implemented and sustained throughout the organisation in conjunction with appropriate User awareness training.
- The vulnerabilities that could be exploited by malware are kept minimum through vulnerability management controls and tactics. This is provided through SecurityJoes.
- Antimalware software scans computers every time and again.

7.3 VIRUS PROTECTION

Users are alerted to the fact that viruses can cause substantial harm to the Company's computer system. The damage caused is often not limited to hardware or software but can result in financial loss to the Company because of lost production. Therefore:

Users are to ensure that the latest Company approved anti-virus protection software has been installed on their personal computer and is permanently enabled.

- Should any data be received by a User via disk, CD ROM, Internet, e-mail or any other external source, a comprehensive scan of that data should be

performed prior to loading that data onto the Company computer system by the company IT department.

- If a virus is detected, the Helpdesk serving at the Company premises should be notified immediately.
- Installation of non-Company approved virus protection software is prohibited.
- Users are under no circumstances to disable the anti-virus software or reconfigure any settings on the anti-virus software unless specifically authorized by the IT Helpdesk or IT Department or Chief Executive Officer of the Company; and
- Users should never distribute virus information e.g., hoax virus e-mails (real or otherwise) to others. If any User encounters virus information, they should forward it to the Helpdesk or anti-virus specialists at their offices or IT Helpdesk.
- Non-company owned computer equipment are not allowed to be connected to the company network without prior written consent and virus scanned by the company IT department.

7.4 BACKUPS

The organisation conforms to a standard backup and recovery control process in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency. In addition, it seeks to define controls to enforce regular backups and support activities, so that any risks associated to the management of data backups and recovery are mitigated.

DATA BACKUP STANDARDS

- Critical data, which is critical to the organisation, must be defined by the Business in consultation with IT and must be backed up.
- Backup data must be stored at a backup location that is physically different from its original creation and usage location (i.e., The Disaster Recovery Site). The medium will dictate when schedule.
- Data restores must at least be tested quarterly.
- Procedures for backing up critical data and the testing of the procedures must be documented by the IT. These procedures must include, as a minimum, for each type of data and system:

- i. A definition of the specific data to be backed up.
 - ii. The type(s) of backup to be used (e.g., full back up, incremental backup, etc.).
 - iii. The frequency and time of data backup.
 - iv. The number of generations of backed up data that are to be maintained (both on site and off site).
 - v. Responsibility for data backup.
 - vi. The storage site(s) for the backups.
 - vii. The storage media to be used.
 - viii. Any requirements concerning the data backup archives.
 - ix. Transport modes; and
 - x. Recovery procedure of backed up data.
 - xi. All data and software essential to the continued operation of the organisation, as well as all data that must be maintained for legislative purposes, must be backed up.
- Backup schedules must not interfere with day-to-day operations. This includes any end of day operations on the systems.
 - When the data in a system change frequently, backups need to be taken more frequently to ensure that data can be recovered in the event of a system failure.

BACKUP TYPES

- Full backups should be run weekly as these datasets will be stored for a longer time. This will also aid in ensuring that data can be recovered with the minimal set of media used at that time. Once a month, a full backup should be stored off site.
- Differential/Incremental backups must be used for daily backups. This ensures that the backup time window is kept to a minimum during the week while allowing for maximum data protection.
- If a system requires a high degree of skill to recover from backup, consideration must be given to making full images of such servers as a backup. This will ensure that the system can be recovered with minimal knowledge of the system configuration.

STORAGE MEDIUM

When choosing the data media format for backups, it is important to consider the following:

- Time constraints around identifying the data and making the data available.
- Storage capacity.

- Rate of increasing data volume.
- Cost of data backup procedures and tools vs. cost if restored without backup.
- Importance of data.
- Life and reliability of data media.
- Retention schedules; and
- Confidentiality and integrity.

OFFSITES STORAGE SITE

- Data backups must be stored in two locations:
 - i. One on-site, or in proximity
 - ii. An off-site location, to additionally provide protection against loss to the primary site and on-site data.
- Off-site backups must be a minimum of 5 kilometres from the on-site storage area to prevent a single destructive event from destroying all copies of the data.
- Should high availability be required, additional backup copies may be securely stored in the proximity of the ICT system (within the data centre or secure vault).
- Minimum requirements are to store the monthly and/or yearly backup sets off site.
- The site used for storing data media off-site must be physically secure and safe.
- Should an off-site media set be required to perform a restore, the data media must be returned to the offsite facility for the remainder of the applicable retention period.
- All data media used to store information must be disposed of in a manner that ensures the data is not recoverable.

RECOVERY OF BACKUP DATA

- Documentation of the restoration process must include:
 - i. Procedures for the recovery
 - ii. Provision for key management should the data be encrypted.
- Recovery procedures must be tested at least quarterly, and Disaster Recovery procedures must be tested at least yearly.
- Recovery tests must be documented and submitted to the Manager.

8.COMMUNICATION SECURITY POLICY

PURPOSE

This policy has been established to protect information as it is transferred within the organisation or to external parties, whether electronically or otherwise. It addresses the requirements for the secure design and management of networks and networking services, electronic messaging, courier services and information exchange arrangements.

8.1 NETWORK CONTROLS

- There shall be segregation of duties between personnel responsible for network implementation and operations and computer implementation and operations.
- Access to networking devices must be controlled in accordance with the Access Control Policy
- All network devices must be configured to log security and related events to the central logging server established for this purpose. Logs are to be retained in accordance with the retention provisions of the Asset Management Policy
- All protocols, ports and services on networking devices must be specifically approved with a business justification in accordance with the change management clauses of the Operations Security Policy and Change Management Process
- Networking devices must be configured in accordance with industry best practices.
- Network Penetration tests shall be performed once per year to ensure that all services in the network are secure. This is done by SecurityJoes, our security operation centre.
- Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

8.2 SEGREGATION IN NETWORKS

- To help contain network security risks and improve security management, groups of information services, Users and information systems must be segregated as follows:
 - i. networks are to be segregated into smaller network domains according to trust level, information classification, organisational units, and functionality.

- ii. Segregation is to be accomplished by using a different VLAN and IP Subnet for every domain.
- iii. The perimeter of each domain must be well defined.
- iv. Access between network domains must be controlled at the perimeter using a firewall.
- v. Implement a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network.
- vi. Implement a DMZ to limit inbound traffic to only system components that provide authorised publicly accessible services, protocols, and ports.
- vii. Limit inbound Internet traffic to IP addresses within the DMZ.
- viii. Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address)
- ix. Place system components that store Restricted data in an internal network zone, segregated from the DMZ and other untrusted networks by firewalls and proxy servers.
- x. Network domains which contain wireless access points must be separated from the rest of the network using firewalls.

8.3 NETWORK DOCUMENTATION

- Network Documentation will be classified Confidential and handled in accordance with the requirements for Confidential information.
- Layer 2 and 3, and Physical diagrams of our networks and information processing environments that identify all connections to external networks must be documented.
- A register of all authorised network devices including routers, switches, hubs, fire walls and wireless access points, and detailing as a minimum: make, model, operating system name, version and patch level, serial number, owner, owner contact details, and dates of last and next device configuration review.
- Comprehensive records of IP addressing and VLAN assignments, including static IP address assignments, indicating for each IP the host VLAN, host device, host name, location, internal FQDN, role, external FQDN, and external (NAT) IP address if any

8.4 MOBILE DEVICES AND TELEWORKING

- Employees must never use personal Mobile Computing and Storage Devices for accessing or processing company Information or Information Systems.
- Employees must never use or provide their personal telephone numbers for carrying out their duties as company employees.
- Restricted and Confidential data stored on mobile devices, including notebook and tablet computers, cell phones, removable storage, and e-readers, must be encrypted.
- Mobile computing and storage devices which contain Information classified Restricted or Confidential must never be left unattended and, where possible, should be locked away or secured with special locks.
- Devices should be equipped with mobile device tracking software to facilitate location or return in the event it is lost or stolen.
- The theft or loss of a mobile computing or storage device must be immediately reported to the IT for resolution.
- When working from home, employees shall make sure all company information assets are secure and out of reach of relatives.
- Company information assets shall be used strictly for company business only.
- The environment of the teleworking site should be as secure as company office facility and the company information being accessed or processed should not be visible or accessible to other people in the environment, including family members.
- When teleworking requires the remote access of Company systems, access must be accomplished by use of an encrypted and authenticated VPN connection that restricts access to just the systems required to accomplish the work at hand.
- When teleworking requirements include the need for handling of physical Information assets, the teleworking site must be equipped with the necessary lockable filing or storage facilities that protect these Information assets to the same extent as they are protected when used in a Company office environment.

- Teleworking must be carried out in a manner which ensures the equipment and services being used cannot be accidentally or intentionally used by family members, visitors, or other members of the public.
- Teleworking which involves information Classified as Restricted or Confidential must be carried out in a manner which ensures the Restricted or Confidential information is not accessible to family members, visitors, or other members of the public.
- Training must be provided, at least annually, to Company teleworkers to raise their awareness of the additional risks of teleworking.

CONFIDENTIAL

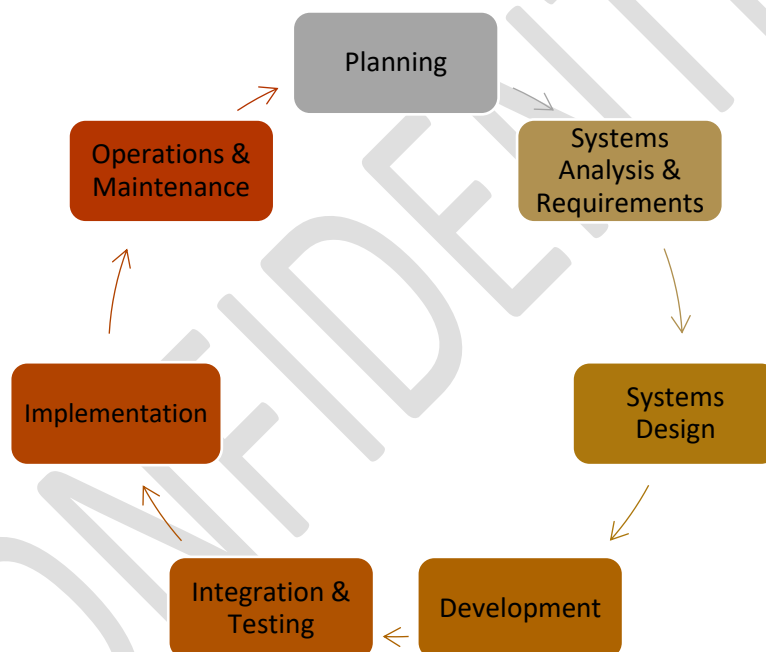
9.SYSTEM ACQUISITION, DEVELOPMENT AND MAINTANANCE POLICY

PURPOSE

This policy has been established to ensure that security is an integral part of Information systems throughout their lifecycle, including those that provide services over public networks, that information security is integrated into the System Development Life Cycle (SDLC), and to ensure the protection of data used for testing.

9.1 SYSTEM DEVELOPMENT CYCLE

A system development life cycle (SDLC), sometimes called a software development life cycle is a term used to describe the methodical and multi-step process by which a newly conceived technical or non-technical project is transformed into an operational system of predictable quality, and which meets or exceeds business expectations.



When developing, acquiring, or making major changes to an Information System, the respective Information Owners must ensure that all necessary security needs are considered right from the initiation of the planning stage, and reviewed at the start of each successive planning stage in the case of iterative SDLC, by:

- Determining and documenting the confidentiality, integrity, and availability requirements of all the Information Assets to be processed or produced by the Information System and of the Information System itself.

- Determining and documenting the processing requirements for access provisioning and authorisation for the various business use roles as well as for privileged use roles
- Documenting security requirements derived from business processes, such as those for logging and monitoring, and non-repudiation.
- Documenting specific procedures and standards that must be used to mitigate risks and safeguard the Information System, or to interface to other Information Systems
- Establishing the requirements for security controls within the System based on a Risk Assessment
- Documenting the roles and responsibilities related to security management of the Information System
- Documenting communication procedures for security-related events and incidents
- Criteria for accepting Information Systems must be defined at the outset, for example, in terms of their functionality and security requirements.
- Information Systems must be evaluated against these criteria before acquisition or after development.

9.2 PROTECTION OF APPLICATION SERVICES TRANSACTION

Information involved in application service transactions must be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

- Transactions which are intended to be legally binding must implement suitable electronic signatures for each of the involved parties.
- The storage of transaction details and static records must not be in any publicly accessible environment. They must be held on a storage platform contained in an interior firewall zone and not retained or exposed in the DMZ accessible from the Internet or other wide area network.
- Identified Security Requirements of every system are always address in the design phase and verified at security checkpoints throughout the SDLC.
- System developers are knowledgeable about secure development practices relevant to their field and subscribe to a professional body with a code of ethics such as OWASP and which keeps them abreast of current best practices.
- Development and configuration are carried out in a secure test environment.

- System developers can avoid, finding and fixing vulnerabilities including those as published from time to time by, the OWASP Guide, SANS CWE Top 25, and CERT Secure Coding which have included, amongst others: injection flaws; buffer overflows; improper error handling; cross-site scripting; cross-site forgery request; and broken authentication and session management.

9.3 SYSTEM CHANGE CONTROL PROCEDURES

Change control within development activities is controlled by the same formal procedures established for operations management by the Operations Security Policy and include:

- Ensuring change requests are submitted by authorised persons.
- Reviewing security and integrity controls to ensure they will not be compromised by proposed changes.
- Ensuring proposed changes are approved by authorised personnel before development.
- Ensuring developed changes are thoroughly tested and receive User Acceptance before implementation.
- Ensuring that system documentation is always updated on the completion of each change.
- Ensuring version control for all software and configuration updates
- Maintaining an audit trail of all change requests
- Ensuring that User documentation and procedures are changed as necessary to remain appropriate.

9.4 OUTSOURCED DEVELOPMENT

Our organisation supervises and monitors all the activity of outsourced developers, and this is built into the supplier contracts along with:

- Licensing arrangements, code ownership, and intellectual property rights related to the outsourced development.
- Contractual requirements for secure design, coding, and testing practices
- Acceptance testing for the quality and accuracy of the deliverables including the established security requirements.
- Contractual right to audit development processes and controls.

- Contractual requirement for adequate documentation of the developed systems or system components.
- Contractual provision for the developers to provide evidence of sufficient testing to guard against the presence of known vulnerabilities and common coding errors.

9.5 SYSTEM SECURITY TESTING AND ACCEPTANCE TESTING

- Testing of security functionality must be carried out during development.
- A schedule of security tests, inputs for each and expected outputs of each must be established after the system security requirements have been document as per this policy.
- These security tests must first be conducted by the developers during development.
- Independent testing must then be undertaken for internally and externally developed systems to ensure that the system works as intended and only as intended.
- The extent of testing should be proportionate to the importance and nature of the system as determine by considering the sensitivity of information assets it processes or produces, and its criticality to business.
- Testing should include the developed components as well as integrated systems and components.

9.6 PROTECTION OF TEST DATA

- Access control mechanisms which apply or would apply to protect operational data must also be applied to the protection of test data.
- Whenever possible operational data should not be used as test data. When it is necessary to use operational data as test data there must be specific authorisation for this every time operational information is copied to a test environment and operational information must be securely deleted from the test environment as soon as testing is completed.
- The copy and use of operational information should be logged and documented to provide an audit trail.

10. INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

PURPOSE

This policy has been established to provide a consistent and effective approach to managing Information Security Incidents including communication on security events and weaknesses. It must be read in conjunction with our security operation centre service provider procedures.

10.1 POLICY STATEMENT

Our organisation has established and maintains mechanisms for identifying, reporting, and recording of Information Security Events and Incidents. In response to business need the organisation has developed and maintains an Incident Response Plan and a 24/7 Incident Response Team to provide swift and competent response when an Information Security Incident is thought to be occurring, or to have occurred.

All Employees, Contractors and Third parties involved in using or accessing organisational Information Systems, Information Assets or Information Processing Facilities are responsible for reporting Security Events including potential or suspected Security Incidents, as soon as possible after discovery, using the “Group Incident Escalation Procedure”.

All security incidents shall be investigated and closed with a resolution being documented.

Our service provider SecurityJoes is responsible for manning 24/7 security environment of our information asset.

11. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT POLICY

PURPOSE

This policy has been established to provide for the continuity of Information Security during adverse situations. There are no times when it would be acceptable to disregard the requirements of the organisation Information Security Policies.

This policy section is referred to the IT Business continuity and disaster recovery policy.

12. DOCUMENT REVIEW

This information security policy shall be reviewed once per year or when there is a change in business processes relating to information security.

REVISION DATE	VERSION	REVISIONS	AUTHOR
25/07/2023	1.1	Including GDPR	Information security officer

13. DOCUMENT APPROVAL

NAME	TITLE	SIGNATURE	DATE