Schauenburg

Information Technology (IT) Policy

Prepared for:	Schauenburg International – Africa Group
Company Discipline:	IT
Author:	Trevor Willemse
Document Number:	POL-09803-R02
Electronic Reference:	SCH-IMS-POL-09803-R02
Effective Date:	25/10/2024
Document Template:	SCH-QMS-TEMP-00005-R06
Site if Applicable:	All

Approval

	Author	Reviewer	Reviewer	Reviewer	Release Authority
Name and Surname	Trevor Willemse	Bruce King	Pierre Geldenhuys	Mark Stevens	Brigitte Pretorius
Title	IMS Coordinator	Business Development Direcotr	Operations Director	CIO	Chief Financial Officer
Date	05-Dec-24	09-Dec-24	05-Dec-24	05-Dec-24	02-Jan-25
Signature	DocuSigned by: Trevor Willemse 61F475D2B5854BA...	Signed by: Bruce King 8CF5885A867F4E0...	DocuSigned by: 9BC10211C12A468...	DocuSigned by: Mark Stevens 9186FCFB9A1642D...	Signed by: Brigitte Pretorius F219C9762E45494...

The responsibility remains with the User to ensure that this document is the latest revision when printed and used.

Schauenburg (Pty) Ltd

Tel: +27 (11) 974 0006
Fax: +27 (11) 974 0077
http://www.schauenburg.co.za
sales@schauenburg.co.za

24/26 Spartan Road
Aeroport Ext 21
Spartan
1619
South Africa

Document Revision History

Revision Number	CP Number	Changed by	Effective Date	Change Order Number and Description of Change
R02		Not Applicable	10/25/2024	New Document released for use. Previous document was not register

Table of Contents

1 THE PURPOSE OF THE DOCUMENT

The purpose of this document is to ensure that:

- Company's information systems are properly assessed for security.
- Confidentiality, integrity, and availability are maintained.
- Employees are aware of their responsibilities, roles and accountability.
- Provide a comprehensive framework that aligns IT practices with organisation goals.
- Ensures compliance with legal and regulatory requirements.
- Promotes security and efficiency, and guides employees in the responsible use of technology resources.

It is a critical document for maintaining operational integrity and safeguarding the organisation's digital assets and reputation.

2 SCOPE

2.1 DOCUMENT OVERVIEW

This document defines all IT policies to ensure clarity and focus on the implementation of information security controls within the organisation and provides a clear definition of what the information security management system covers. It ensures that information security measures are appropriately tailored to the organisation's needs, risks, and operational context, thereby safeguarding information assets and supporting business objectives effectively.

3 INFORMATION SECURITY POLICY

3.1 PURPOSE

The purpose of this policy is Information Security Policy is to establish and maintain framework for managing information security at the organisation in accordance with ISO27001. This policy aims to protect the confidentiality, integrity and availability of information by implementing effective security controls and procedures.

This policy is communicated through the Information Security Policy Statement (POL-09924).

3.2 SCOPE

This policy applies to all employees, contractors, and third-party vendors who have access to the organisation's information assets, including physical and digital information.

3.3 INFORMATION SECURITY OBJECTIVES

- **Confidentiality**: To ensure that information is accessible only to those authorised to have access.
- **Integrity**: To safeguard the accuracy and completeness of information and processing methods.
- **Availability**: To ensure that authorised users have access to information and associated assets when required.
- **Validity**: to ensure obsolete data is deleted and only the current version of information is retained, unless historical changes are required. Follow documentation retention period process.

3.4 ROLES AND RESPONSIBILITIES

- **Information Security Manager**: Responsible for overseeing the implementation, monitoring, and maintenance of the information security management systems (ISMS).
- **Top Management**: Responsible for supporting ISMS, providing resources, and ensuring alignment with organisation objectives.
- **Employees and Contractors**: Responsible for adhering to the information security policies and procedure.
- **IT Support Company**: Responsible for ensuring the availability, managing and resilience of the company's infrastructure and assets, as well as implementation and maintaining appropriate security arrangements for IT administrative access and security controls.

3.5 INFORMATION SECURITY RISK MANAGEMENT

- **Risk Assessment**: Regularly conduct risk assessments to identify, evaluate, and prioritise risks to information security.
- **Risk Treatment**: Implement appropriate controls to manage identified risks in line with the risk assessment results.

3.6 SECURITY CONTROLS

- **Access Controls**: Ensure that access to information and information systems is restricted to authorised users only.
- **Data Encryption**: Use encryption to protect sensitive data both in transit and at rest.
- **Incident Management**: Establish procedures for reporting and responding to information security incidents.
- **Business Continuity**: Develop and maintain business continuity plans to ensure that critical information and systems can be restored following a disputation.

3.7 COMPLIANCE

- **Legal and Regulatory Requirements**: Comply with applicable laws, regulations, and contractual obligations related to information security.
- **Internal and External Audits**: Conduct regular audits to ensure compliance with the information security policy and ISO 27001 requirements.

3.8 POLICY REVIEW AND REVISION

- **Review Frequency**: The Information Security Policy will be reviewed at least annually or when significant changes occur to the organisation or its information systems.
- **Revision Process**: Updates to the policy will be documented and communicated to all relevant parties.

3.9 TRAINING AND AWARENESS

- **Training Programs**: Provide regular information security training to all employees and contractors to ensure awareness and compliance with security policies.
- **Awareness Campaigns**: Implement ongoing awareness campaigns to keep information security at the forefront of employees' minds.

3.10 ENFORCEMENT

- **Disciplinary Actions**: Non-Compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual agreements.

4 COMPUTER UPDATE AND MANAGEMENT POLICY

4.1 PURPOSE

This policy outlines the managed configurations for company-owned computers and subsidised laptops, in line with ISO 27001 standards.

4.2 SCOPE

This policy applies to laptops owned and/or subsidised by the company, used by either employees or contractors. Exceptions may apply with approval of director and Chief Financial Officer.

4.3 OWNERSHIP AND RESPONSIBILITIES

The Chief Financial Officer is responsible for overseeing the implementation of this policy.

Employees and authorised third parties are responsible to familiarizing themselves with this policy and ensuring compliance with this policy's requirement.

4.4 GENERAL CONFIGURATION GUIDELINES

4.4.1 DOMAIN MEMBERSHIP

Computers which are the primary office computer of the owner shall be joined to the company Domain and will therefore be managed per the "Managed Configuration" section below.
Laptops which are intended to be a shared resource, primarily among employees with a company login account will also be managed per the "Managed Configuration" section below. This includes departmental and checkout units.

Laptops which are not primary office computers, and which are used by only one individual will be joined to the company Domain. These units will comply with the "Managed Configuration" section below.

4.4.2 MANAGED CONFIGURATION

The following configuration guidelines will be applied to laptops joined to the company Domain:

- Domain: Computers and laptops owned and/or subsidised by the company will be joined to the company domain.
- Username and Password: Managed computers must be logged onto with a given company login ID before it is taken outside of the Company's Head Office Building for that given ID to work outside of the building.
- Windows Update: Windows Update will be forcibly configured to download updates as they become available and installed autonomously by the IT support company. If the installation has been missed, the installation will begin 5 minutes after the unit is available to install updates. If a reboot is required once the installation is complete, the user will be prompted to do so.
- Antivirus Software: Antivirus software will be forcibly controlled by the IT support company and will receive updates as soon as they become available.

4.5 ENFORCEMENT

Any configuration found to conflict with this policy will be corrected autonomously by the IT support company. IT support company shall inform the information officer of such occurrences. The IT support company reserves the right to run robotic scans against managed computers to verify this configuration. Where a computer cannot be corrected autonomously, action will be taken to stop the computer accessing the domain.

4.6 REQUIREMENTS

For this policy to be effective, all company owned and subsidised computers will need to meet the minimum recommended requirements as per the minimum requirements policy from the IT support company. Computers that do not meet the minimum requirements will not be joined to the domain. Exceptions may apply.

5 ACCOUNT RETENTION

5.1 PURPOSE

The purpose of this policy is to define the length of time that company login accounts and associated services will be maintained after the account holder leaves the company. It subsequently serves to maintain the security, operational cost, and efficiency of the company network

5.1.1 SCOPE

This policy applies to all employees and contractors of the organisation, who have login accounts on the organisation's network.

5.2 POLICY

Company network login accounts and associated services (email, file storage, etc…) will be maintained for 30 days after the account holder leaves the employ of the company. After which, the login account, associated email and personal network storage space (S: drive and/or U: drive) will be backed up and deleted.

Exception to this would be for Stratosat only where the account will be maintained for 120 days.

5.3 OWNERSHIP AND RESPONSIBILITY

5.3.1 SUPERVISOR/PEOPLE LEADER

It is the employee's supervisor's or direct people leader's responsibility to submit an account deletion request at least 5 business days before the account holder's last day of service.

In exceptional cases, a supervisor may request access to the emails or files of a departing employee within the defined retention period. Such requests must receive approval from the Information Security Officer or CFO. Once approved, the IT support company will assist the supervisor in accessing the necessary work-related information and data.

5.3.2 ACCOUNT HOLDER

It is the employee's responsibility to ensure that they have copies of any desired personal data (email, contacts, S: drive, etc.) before their last day of service.

The employee is prohibited from making copies of proprietary company information.

5.3.3 IT SUPPORT COMPANY

It is the IT support company responsibility to lock/re-route the account by close of business on the last day the employee is with the company. It is the IT support company's responsibility to backup and delete the account holder's login account and data after the 30/120(Stratosat) working days has expired. This includes VPN access.

5.4 MONITORING

The IT support company will periodically run robotic scans to identify accounts that may no longer be in use (accounts not logged onto after 30/120 days). Departments will be notified if such accounts are found in their department allocation within the company.

5.5 ENFORCEMENT

The system administrator or their delegate will be notified of violations of this policy, at which point they may attempt to work with the department directly. If these attempts are not successful, violation information may be passed along to the CFO of the company for resolution.

6 COMPANY WEB POLICY

6.1 INTRODUCTION AND PURPOSE

The company's World Wide Web presence for public access web pages promotes company activities by providing current and effective interactive communication and online services to a wide audience with the goals of assisting and building broad-based support for the company's products and services.

The purpose of the company's Web Policy for public access web pages is to ensure security, availability, confidentiality, accuracy, consistency, integrity, and protection of the identity and image of the company by aligning with ISO27001 standards for information security, and to define responsibilities and procedures for website management and maintenance.

General oversight of the company's public access web pages, and policies governing the use of these resources, is the responsibility of the Marketing department and the Head of Communications & Facilities.

6.2 SCOPE AND AUDIENCE

The decentralized nature of the World Wide Web and the diverse purposes and constituencies served by the company's websites require that as much freedom as possible be granted to those creating and maintaining websites. However, contents of all Web pages under the company's jurisdiction (i.e., provided by company servers or by other servers funded by the company) must comply with local laws, and with the company's policies, rules, and regulations. Further, the reputation and image of the company is determined, in part, by the quality of information published electronically by its employees and affiliations.

6.3 POLICY

6.3.1 WEBSITE DESIGN AND SECURITY MEASURES

All pages that reside on the company's public access website must adhere to layout requirements and guidelines. These have been formulated to make the information viewable by as large an audience as possible, to make navigation clear to web visitors, to provide contact information, and to regulate the use of the company's logos, wordmarks, and trademarks.

Websites shall implement appropriate security measures, including but not limited to:

- Access controls to ensure only authorised personnel can modify or add content.
- Encryption of sensitive information to protect data in transit and at rest.
- Regular vulnerability scans and patch management for web applications and server configurations.
- Incident monitoring and logging to detect and respond to security incidents promptly.
- Compliance with global data protection regulations, including the GDPR and the POPI Act.
- Secure data handling practices to ensure the confidentiality, integrity, and availability of personal information.

The company is committed to protecting personal information in accordance with the Protection of Personal Information Act (POPI Act). This includes ensuring that personal data collected through the website is processed lawfully, stored securely, and only used for its intended purpose. Users must be informed about the collection and use of their data and their rights to access, correct, or delete their information.

6.3.2 PERSONAL WEBSITES

The company servers are not to be used for hosting personal sites. If you are experiencing issues connecting to the internet, please contact IT support company.

6.3.3 WEBSITE CONTENT CREATION

Please note that any content submitted for publication is subject to approved by the Head of Communications and Facilities.

6.3.4 PROHIBITED CONTENT

6.3.4.1 ADVERTISING

Company web pages may not contain advertising for commercial sites without advance written approval by at least two directors, with one been the director responsible for the portfolio/department. Approval will be considered only if:

- The purpose of the advertising or link is consistent with the Company's mission,
- The advertising or link is essential to the purpose of the site, and
- The advertising or link does not imply Company endorsement of the product or service.

6.3.4.2 EXPLICIT CONTENT

Company webpages must not contain nudity, sexually explicit material, racial content, profanity, hate speech or discriminatory language.

6.3.5 COPYRIGHT MATERIAL

Company webpages may not contain material that is copyrighted without proof of approval of the copyright holder. Copyrighted material that is posted online will follow the rules set out in the copyright.

6.3.6 OUTSOURCING

When arranging for projects to be published on the Company's resources to be produced by an agency outside the department (i.e., outsourcing), it is important to present a clear set of standards and expectations to the external agency or contractor.

Department Responsibilities

- Oversee contractor's implementation and monitor activities.
- Define the relationship between the department and the agency and relay this to the Company's Management.
- Give the company's style and design guidelines to the agency.
- Promote awareness of external agencies or contractor's activities.
- Check webpages for accuracy, currency, and accessibility and suggest improvements. Provide examples of page design and navigation tools that are used on Company webpages.

External Agency or Contractor Responsibilities

- Adhere to the company's style guide and design policy.
- Generated the product as per service/contract agreements.

6.3.7 RESOURCE REGISTRATION

6.3.7.1 WEB SERVER REGISTRATION

All Web service providers are responsible for the currency, legitimacy, legality, and appearance of their pages.

6.3.8 VIRTUAL DIRECTORIES

All use of Virtual Directories within other publications (Newsletters, etc.) should first be cleared up by subject matter expert. Sometimes the preferred virtual directory name is not available.

6.3.9 VIDEO

6.3.9.1 FLASH VIDEO SPECIFICATIONS

All videos must be converted to a company-approved format, such as but not limited to MP4, AVI, and MOV, before being uploaded to the company's web server. Furthermore, it is imperative that each video complies with the required security measures to ensure the protection of company information.

6.3.9.2 CLOSED CAPTIONING

All videos uploaded to the company's web server should have synchronised captioning provided for video or audio presentations.

6.3.9.3 AUDIO DESCRIPTIONS

Supplementary audio information must be provided for video and multimedia presentations if the video depicts information that is not audible.

6.3.9.4 VIDEO CONTENT

For a video to be posted on the company website, its content must be directly related to the company. Marketing department has the right to refusal and will not allow inappropriate video content to be posted.

Consent shall be obtained from any customer/supplier/employee/contractor before publishing any video content in which they may appear.

6.3.9.5 VIDEO PRODUCTION

When arranging for video projects to be produced by an agency outside of the company, it is important to present a clear set of standards and expectations to the external agency or contractor.

Departments responsible

- Oversee contractor's implementation and monitoring activities.
- Define the relationship between the department and the agency, relay this to the Marketing department.
- Give the video policy to the agency.

External Agency/Contractor responsible

- Adhere to the company web policy
- Create a zip file that includes:
    - The video flash file (.flv)
    - Timed Text (TT) xml file
    - MP3 secondary audio file (if applicable).

6.4 ENFORCEMENT

Communications department will review all content and videos before publishing them on the company web servers. If found not to be complying, then it will not be published.

7 DATA RESTORATION POLICY

7.1 PURPOSE

Ensure timely and secure data restoration to minimise business impact. Follow ISO27001 standards for information security during this process. The policy's purpose is to ensure data discretion in restoration requests due to the resources required. IT support companies must have a documented procedure outlining the data restoration steps.

7.2 SCOPE

This policy applies to all requests for data restoration, including but not limited to network drives and email storage.

7.3 POLICY

7.3.1 OWNERSHIP AND RESPONSIBILITIES

- IT support company will not perform any data restorations without approved requests.
- Individuals requiring data restorations must submit a support ticket as completely as possible and approved by manager or director shall be attached to the support ticket.
- CFO will submit the approved requests to the IT support company, when the data restoration involves more than one individual’s data, that it will make every reasonable attempt to recover the data as requested.

7.3.2 DATA RESTORATION PROCEDURES

IT support companies shall follow its own data restoration procedures and shall align with the following:

- Identification: Quickly identify the need for data restoration, including types and extend of data restoration.
- Prioritisation: Prioritise data restoration based on critically and impact on business operations.
- Validation: verify the integrity and completeness of restore data through testing and validation procedures.
- Documentation: Maintain accurate records of all data restoration activities, including timelines and outcomes.
- Verification: verifications of access controls have been correctly restored to any data.

7.3.3 SECURITY CONTROLS

- Implement robust security measures during data restoration to protect sensitive information.
- Ensure data confidentiality, integrity, and availability are maintained throughout the process.

7.4 INCIDENT RESPONSE

Integrate data restoration procedures with the organisation’s incident response plan to facilitate timely recovery from data loss incidents. The IT support company and/or system administrator will follow the incident response guidelines as per IT support company procedures.

8 EQUIPMENT MOVES

8.1 PURPOSE

The purpose of this policy is to ensure correct operation of the Company's information technology resources, to maintain a computing environment that is conducive to conducting business, to maintain an accurate inventory of Company resources in the Information Technology Services inventory system, and to prevent damage to Company computer equipment. This is also aligning with the ISO27001 standards involves comprehensive planning and adherence to critical security measures during these moves.

8.2 SCOPE

This policy is specifically targeted at computer equipment owned, operated, and maintained by the Company. The term "computer equipment" is inclusive of servers, computers, monitors, printers, and other computer accessories.

If you are unsure if a device falls into this category, an inquiry can be submitted to the IT support company.

8.3 POLICY

All cross-office computer equipment moves will be performed by the IT support company. Finance shall be informed of such equipment moves to maintain the asset register.

It is acceptable for an employee to move their own equipment within the same office location without the approval or help from the IT support company.

8.3.1 ROLES

- **IT Support Company**: Responsible for coordinating and overseeing equipment moves.
- **Facilities Management**: Ensures physical infrastructure readiness at destination.
- **Business Unit (BU) Manager**: Ensures that all equipment moves are approved.
- **Finance**: responsible for maintaining the asset register.
- **End Users**: Responsible for preparing equipment and cooperating during the move.

8.3.2 OWNERSHIP AND RESPONSIBILITIES

- It is the responsibility of the user to ensure that a request has been submitted to the helpdesk at least two business days prior to the needed move date. Requests can be submitted via e-mail.
- BU will approve the equipment move
- The helpdesk staff will make all reasonable attempts to facilitate the computer equipment move request.
- The Finance department will make updates to the inventory system and to the computer equipment's network identification information as required by the equipment move request.
- Facilities and IT support company to review and determine if any infrastructure changes are required such as network point locations and power supply.
- Request will be closed off once the equipment move has been completed.

8.4 MONITORING

Compliance with this policy will be established via the scheduled audits on the asset register.

8.5 ENFORCEMENT

Failure to comply with this policy may result in the loss of support for this equipment.

9 SOFTWARE LICENCE TRANSFER POLICY

9.1 PURPOSE

This policy outlines the procedures and guidelines for transferring software licenses from one user to another within the company. The goal is to ensure compliance with software licensing agreements and to maintain accurate records of software usage

9.2 SCOPE

This policy applies to all employees, contractors, and third parties who use company-owned software licences.

9.3 POLICY

9.3.1 ELIGIBILITY FOR TRANSFER

- Software licences can only be transferred between users within the company.
- The transfer must be approved by the department manager and the IT support company.

9.3.2 REQUEST FOR TRANSFER

- The current user or manager must submit a request to the IT support company.
- This request must include the details of the software, the current user and new user.

9.3.3 APPROVAL PROCESS

- The IT support company will review the request to ensure compliance with the software licence agreement.
- The department manager must approve the transfer request.
- If approved, IT support company will update software licence records and notify both users of the change.

9.3.4 RESPONSIBILITIES

- The current user or manager is responsible to ensure the software and related data are properly backed up before the transfer.
- The new user is responsible for arranging the software installation and functions correctly.
- The IT support company is responsible for maintaining accurate records of software licences and ensuing compliance with licences agreements.

9.3.5 COMPLIANCE

- All software transfers must comply with the terms and conditions of the software licence agreement.
- Unauthorised transfer or use of software licences is strictly prohibited and may result in disciplinary action.

10 EQUIPMENT/SYSTEMS PURCHASE POLICY

10.1 PURPOSE

The purpose of this policy is to ensure technology equipment being purchased with company assets is compatible with existing company equipment, purchased and deployed in an acceptable timeframe, is

purchased from a reputable manufacturer, has a warrantee and fits within the company and IT support company guidelines. All equipment purchased shall align with the ISO27001 standards requirements.

10.2 SCOPE

This policy applies to all departments and personnel involved in the acquisition of IT and related equipment with organisation's funds.

10.3 POLICY

All purchases of computer hardware or software will be coordinated with management.

10.4 OWNERSHIP AND RESPONSIBILITIES

- **IT Support Company**: Responsible for evaluating the security implications of proposed equipment purchases and ensuring compliance with ISO27001 standards. IT support company should provide a detailed equipment list with the input of requestor. Also responsible to confirm compatibility before purchasing, as well the risk assessment and treatment plan update.
- **Procurement**: Responsible for using the detailed equipment list and provide a quote for the IT support company and the requestor.
- **Finance Department**: Updating and maintaining the asset register.
- **End User**: Responsible providing input on functional requirements, to get approval to purchase equipment, and collaborating with IT support company. When receiving the equipment, the end user must provide details to the finance department for the asset register. End user shall be responsible to return previous company laptop once they have confirmed all required information and data has been moved onto the new laptop.

10.5 EQUIPMENT/SOFTWARE SELECTION CRITERIA

- Equipment/Software must meet with specifications security requirements outlined in existing agreements with the IT support company, including encryption capabilities, access controls, and vulnerability management.
- Equipment/software will be compatible with existing IT infrastructure and systems must be verified. If this cannot be achieved, then director approval shall be required and feasible solution to be found. IT support companies with the requesting department will ensure there is a workable solution that may need to be considered during this period.

10.6 RISK ASSESSMENT

- Conduct risk assessment to identify potential security risks associated with the new equipment or systems acquisitions.
- Mitigate identified risks through appropriate security measures and controls.

10.7 ENFORCEMENT

Non-compliance with this policy will result in equipment or systems not been supported by IT support company and may also result in disciplinary action.

11 NETWORK STORAGE POLICY

11.1 PURPOSE

The organisation provides essential network storage to all organisation employees and contractors. The most prominent of these are file server storage space and email service. These services are extremely valuable due to their availability from virtually any internet-connected computer, and the fact that information stored on them is backed up on a regular basis. Because of this, we encourage everyone to make full use of these resources for work-related information.

However, as stewards of this information we must manage unchecked, disproportional, and abusive use of these resources. Therefore, we allocate reasonable quotas, each working slightly differently. Note that these are not absolute bounds – you are welcome to request an increase in allotment, but this is subject to a robotic, categorical review of the data currently being stored.

Only business-related information and documents are permitted to be stored on the company's servers and cloud services.

Users should keep only the most current files and data, removing outdated versions unless they are required historical reference. This practice helps ensure adequate storage capacity for essential files and data. Historical files documenting changes and developments over time may be preserved for reference purposes.

11.2 SCHJHBDC01

Shared folders and restricted folders will be monitored and reports to be generated quarterly to check security access on all folders.

If you have questions or comments about the policy, submit a service request at the helpdesk.

12 PERSONAL FOLDER PERMISSIONS POLICY

12.1 PURPOSE

The purpose of this policy is to:

- Ensure that personal folders are accessed only by authorised individuals.
- Protect sensitive and confidential information.
- Support the organisation’s ISMS in compliance with ISO27001 and applicable regulations.

12.2 SCOPE

This policy applies to all employees, contractors, and third parties who have access to personal folders as well as emails on the organisation’s information systems.

12.3 DEFINITIONS

- **Personal Folder:** A directory or storage location assigned to an individual for storing personal or work-related data.
- **Company Shared Drive:** A centralised storage system where employees can collaboratively store, access and manage work-related information and documents.
- **Access Control:** Mechanisms used to restrict access to information systems and data based on user identity and authorised level.

12.3.1 ROLES AND RESPONSIBILITIES

- **Information Security Manager:** Oversees the implementation and enforcement of the policy.
- **Information Officer:** Person appointed in accordance with the POPI and PAPI act.

- **IT support company:** Manages technical aspects of access control and permissions.
- **Managers and Supervisors:** Ensure that their team members adhere to the policy and request necessary permissions.
- **Employees:** Comply with the policy and report any access issues or breaches.

12.4 POLICY

Changes to a personal folder will only be made with the owner's consent.
Users are required to use their personal network data drive responsibly. No illegal or inappropriate material shall be stored on these drives. Additionally, work-related files should not be shared from personal drives.

Exception: If illegal or inappropriate content is found during a routine scan by the IT support company, the owner's consent will be overruled, and management will be notified. This will be investigated. Users should only store work-related files and data.

If the information owner is no longer an employee of the company, and the information needed is deemed to be vital to the business operations of the department, a request must be made in writing by the department head requesting access to specific files or folders within 10 working days. Exception to this would be for the Stratosat group that the IT support company will arrange that data will be made available via a shared drive.

12.4.1 ACCESS CONTROL

- **Principle of least privilege:** Access to personal folders should be granted based on the minimum necessary permissions required for the performance of job duties.
- **Authorisation:** Access to personal folders must be authorised by the relevant manager.
- **Access Review:** Regular reviews of folders permissions should be conducted to ensure appropriateness and compliance.

12.4.2 USER AUTHENTICATION

- **Strong Authentication:** Access to personal folders and emails must require strong authentication methods as complex passwords or multi-factor authentication (MFA)

12.4.3 PERMISSIONS MANAGEMENT

- **Role-Based Access Control (RBAC):** Assign permissions based on the user's role within the organisation.
- **Temporary Access:** Any temporary access to personal folders must be explicitly approved and time limited.
- **Revocation:** Access rights must be promptly revoked when an employee leaves the organisation or changes roles.

12.4.4 DATA PROTECTION

- **Confidentiality:** Personal folders containing sensitive information should be encrypted both in transit and at rest.
- **Data Handling:** Users must handle personal folder data in accordance with the organisation's data protection policies and procedures.

12.4.5 MONITORING AND AUDITING

- **Incident Reporting:** Any suspected breach or violation of folder permissions must be reported immediately to the information security manager as well as the information officer as per POPI.

12.5 ENFORCEMENT

- **Violations:** Non-compliance with this policy will result in disciplinary action, up to and including termination of employment.
- **Exceptions:** Any exceptions to this policy must be formally requested and approved by the Information Security Manager/CFO and department director

13 DEPARTMENT SHARED SERVER SPACE POLICY

13.1 PURPOSE

The purpose of this policy is to:

- Ensure that acceptable use of shared storage space on organisation's server for integrity of business resources
- Protect sensitive and confidential information.
- Support the organisation's ISMS in compliance with ISO27001

13.2 SCOPE

This applies to all employees and contractors of login accounts.

13.3 DEFINITIONS

- **Department Shared Drive:** A shared network drive designated for departmental use, providing centralised storage for departmental files and resources.
- **Access Control:** Measures to restrict access to information and data based on user roles and permissions.
- **Data Protection:** Measures to ensure the confidential, integrity and available of data.
- **S Drive:** This is the common general network drive that all users have access to.

13.3.1 ROLES AND RESPONSIBILITIES

- **Information Security Manager:** Oversees the implementation and enforcement of the policy.
- **Information Officer:** Person appointed in accordance with the POPI and PAPI act.
- **IT Support Company:** Manages technical aspects of access control and permissions.
- **Managers and Supervisors:** Ensure that their team members adhere to the policy and request necessary permissions.
- **Employees:** Comply with the policy and report any access issues or breaches.

13.4 POLICY

Every department has a shared space on the organisation's server, which is restricted to members of their department. This is located under "Restricted Folder Access".

When collaborative work requires shared access to files/folders on the server, the S Drive shall then be used. Under no circumstances are user directories to be used for shared access.

It is prohibited from saving sensitive or confidential information on the general S Drive.

13.4.1 GENERAL CONFIGURATION GUIDELINES

- Each department has designated space on the network.

- All members of a given department shall have read and write access to that directory/folder.
- Exceptions will be made for organisation's share information where all users will have Read Only access to the directory/folder such as but not limited to Training documents, Policies, Procedures.
- At any given time, no user shall have access to the restricted directories/folders without prior written approval from department manager.
- Access permissions should be reviewed at least annually to ensure they remain appropriate.

13.4.2 DATA PROTECTION

- **Confidentiality**: Sensitive Data shall not be stored on the S Drive, this data shall be stored on either the departmental directory/folder or the users personal storage space.
- **Backup**: Regular backups of the servers will be conducted to ensure data restoration in case of loss or corruption. Backup schedules will be aligned with the business-critical requirements.

13.5 MONITORING

- **IT Support Company**: IT Staff shall review security configuration of network resources, including but not limited to, granted access to servers.
- **Incident Reporting**: Any suspicious activity or policy violations must be reported immediately to the information security manager as well as the information officer as per POPI.
- **Compliance:** Any configuration that conflicts with this policy shall be replaced or reset. The account holder should be notified, depending on the situation. If data loss occurs during the replacement or resetting process, the account holder shall be informed, provided data restoration does not compromising the security of other account holders.

13.6 ENFORCEMENT

- **Violations:** Non-compliance with this policy will result in disciplinary action, up to and including termination of employment.
- **Exceptions:** Any exceptions to this policy must be formally requested and approved by the Information Security Manager.

14 INFORMATION CLASSIFICATION POLICY

14.1 PURPOSE

The purpose of this policy is to ensure that information is classified appropriately to protect its confidentiality, integrity, and availability, in alignment with ISO27001 requirements.

14.2 SCOPE

This policy applies to all employees, contractors, and third-party users who have access to the organisation's information assets.

This policy covers all types of information such as but not limited to electronic files, hard copy documents, emails and applies to all departments, employees, contractors and third-party users.

14.3 INFORMATION CLASSIFICATION LEVELS

- **Unrestricted:** Information that is intended for and could be released to public dissemination and requires the lowest level of information security.

- **Internal/Company Restricted:** Information that is restricted to internal use within the organisation and should not be disclosed to outside parties without proper authorisation.
- **Confidential/Company Confidential**: Information that is sensitive and requires a higher level of protection. Unauthorised disclosure could significantly harm to the organisation or its stakeholders.
- **Company Secret:** Information that is highly sensitive and requires the highest level of protection. Unauthorised disclosure could cause sever harm to the organisation or its stakeholders

14.4 Labelling and Handling

All information assets must be labelled according to their classification. The following guidelines should be followed:

- **Public:** Marked as “Unrestricted” or no special labelling required.
- **Internal:** Marked as either “Internal” or "Company Restricted".
- **Confidential:** Marked as either “Confidential” or "Company Confidential".
- **Highly sensitive:** Marked as "Company Secret”.

14.5 Access Control

Access to information assets should be granted based on the principle of least privilege. Only authorised individuals should have access to information based on their role and responsibilities.

14.6 Information Transfer

Information transfer rules and procedures must be in place to ensure secure transfer of information within the organisation and with external parties. This includes physical transfers, electronic transfers, and verbal communication.

14.7 Training and Awareness

All employees, contractors, and third-party users must receive training on information classification and handling procedures. Regular awareness programs should be conducted to reinforce the importance of information security.

15 Network Support Equipment Policy

15.1 Purpose

Define the objectives of the policy, such as ensuring the security, availability, reliability and integrity of network support equipment and network infrastructure. By implementation and maintaining appropriate support equipment and redundancy measures for business-critical functions and systems. This policy will better reduce destructive equipment activities on the organisation’s network and minimize the risk of loss of data, time and resources.

15.2 Scope

Specify which equipment, locations, and personnel the policy applies to, including routers, switches, firewalls, load balancers, and other network hardware components used within the company’s IT infrastructure.

15.3 Definitions

Network Support Equipment: including definitions of all relevant terms and equipment to ensure clarity.

15.4 POLICY

Aims to protect network support equipment from security threats, ensuring operational continuity and compliance with ISO27001.

All network equipment in use at the organisation shall be owned by the organisation and administered by the IT support company. Exceptions may be made for approved client-owned equipment, provided that the IT support company determines that such equipment does not compromise the network.

Employees/Contractors are prohibited from providing their own networking equipment. If the organisation's resources do not meet your networking equipment needs, please submit a new equipment request to the IT support company. The organisation will strive to fulfil reasonable requests for additional networking equipment.

15.4.1 ROLES AND RESPONSIBILITIES

- **IT support company and network teams:** Responsibilities for the configuration, management, and monitoring of network support equipment. Conducting regular reviews of this equipment and advise of any equipment reaching end-of-life.
- **Chief Financial Officer:** Oversight of security measures and compliance with the policy.
- **Management:** Ensure adequate resources and support for policy implementation.
- **Department Appointed employees:** employees appointed to perform similar duties as the IT support company and network teams due to business needs and activities.

15.4.2 GENERAL CONFIGURATION GUIDELINES

Company supplied network support equipment shall be configured and/or by the IT support company, this would include any privately owned network support equipment (approved by exception). Administrative rights to all network support equipment will be retained to the IT support company.

15.5 EQUIPMENT REDUNDANCY

Redundancy must be in place for any business-critical functions and systems to ensure high availability and minimise downtime. This includes having backup equipment and failover mechanisms to handle hardware failures or other disruptions.

15.6 MONITORING

All network support equipment must be regularly maintained and monitored to ensure optimal performance and early detection of potential issues. This includes routine inspections, firmware updates and performance checks. This may be carried out by either IT support company or department appointed employees.

The IT support company shall perform unscheduled network sweeps with the intention of discover non-compliant equipment.

The IT support company will regularly review equipment and inform the company when any equipment is nearing end-of-life.

Enable logging on network support equipment to capture relevant events and activities.

Implement monitoring tools to detect and respond to anomalies or unauthorised activities.

15.7 MAINTENANCE AND UPDATES

Network equipment owner shall arrange and regularly apply security patches and updates to network support equipment.

Schedule regular maintenance to ensure equipment remains in optimal condition.

15.8 Incident Response

In the event of a network equipment failure, IT support team must follow established incident response procedures to quickly restore normal operations. This includes utilising redundant equipment and failover systems as necessary.

15.9 Physical Security

The IT support company, except in certain instances where the department is involved, must maintain controlled access to network support, monitoring equipment, and environments. Additionally, it must safeguard against environmental hazards.

15.10 Compliance and Audits

Ensure compliance with ISO27001 requirements and other relevant regulations.

Conduct regular internal and external audits to assess adherence to the policy and identify areas for improvement.

16 Non-Company owned Equipment Support Policy

16.1 Purpose

To establish guidelines for managing and securing non-company owned equipment that interacts with or is used in conjunction with the organization's IT infrastructure.

Company and IT support company has limited resources and therefore stay focused on organisation's assets subject to their scope of work and or area of responsibility. It is understood that some employees and contractors are authorised to use their private computer equipment to conduct company's business.

16.2 Scope

Applies to all non-company owned equipment used within the organization's network or systems, including personal devices, contractor equipment, and third-party hardware.

16.3 Definitions

Non-Company Owned Equipment: Any hardware or device not owned by the organization but used within its environment, including personal laptops, smartphones, tablets, and contractor or vendor-provided devices

16.4 Policy Statement

To ensure that non-company owned equipment used in the organization's environment meets security requirements and does not compromise the integrity, confidentiality, or availability of organizational information.

Employee should always save organisation's data and information onto the organisation's servers whenever possible.

Non-company owned equipment shall be authorized before connection to the organization's network or systems. Authorization requests must be submitted to and approved by the department head or designated authority.

16.4.1 Security Requirements

Non-company owned equipment must adhere to the organization's access control policies. This includes requiring strong authentication methods and restricting access to sensitive information based on user roles and need.

Non-company owned equipment must have up-to-date antivirus and anti-malware software installed.

All sensitive data on non-company owned equipment must be encrypted according to the organisation's encryption standards.

16.4.2 SUPPORT

Employee and contractor will need to grant the IT support company permission to perform work on the private owned equipment by submitting the required request stating their support for this work. The organisation has the right to decline such activities.

16.4.3 EXITING ORGANISATION

Upon the circumstances that an employee or contractor will no longer be employed by the organisation, the employee/contractor shall be responsible to first remove all organisation's data and information.

The employee shall grant permission to the IT support company to conduct a detailed audit of this equipment to ensure that all organisation's data and information has been removed from the equipment.

Any organisational data stored on non-company owned equipment must be securely deleted before the equipment is disconnected or returned.

16.5 ENFORCEMENT

Supervisor/Manager is responsible for enforcing this policy, authorizing equipment connections, assisting with configuration, and managing incidents related to non-company owned equipment.

17 PASSWORD POLICY

17.1 PURPOSE

Passwords can be classified as weak or strong based on how difficult they are to guess and/or compute. The Company password policy has been chosen as acceptable by the administrators to offer a level of protection beyond simple or weak but not to be so complex as to require being written down and causing additional risk.

17.2 SCOPE

This policy applies to all employees, contractors, and third-party users who have access to the organisation's information systems and data.

17.3 DEFINITIONS

Password: A string of characters used to authenticate a user's identity and access information systems or data.

17.4 POLICY

17.4.1 PASSWORD CREATION

Complexity Requirements: Passwords must meet the following complexity requirements and must contain characters from at least three of the following 5 categories:

- Minimum Length of 8 characters.
- English uppercase characters (A – Z)
- English lowercase characters (a – z)
- Non-alphanumeric (For example: $, #, or %)
- Passwords shall not contain the first name, last name, or username of account in question

17.4.2 PASSWORD MANAGEMENT

Passwords must be changed every 90 days. Users will be notified to change their password before it expires.

Do not reuse any of your last 4 passwords.

Passwords must be securely stored using strong encryption. Do not write down or store passwords in plaintext.

Exceptions exist for specific company systems accessible only through the secured network.

17.4.3 Password Protection

Passwords must be kept confidential and should not be shared with others.

Accounts will be locked after 5 unsuccessful login attempts to prevent brute-force attacks. Locked accounts can be unlocked by contacting the IT supply companies or the relevant application company system administrator.

Sharing passwords is strictly prohibited. Users must not use another person's password, even with permission.

17.4.4 Password Reset and Recovery

Password resets must be conducted through secure channels. Users must verify their identity through multi-factor authentication (MFA) before a password reset is processed.

Users must utilize self-service password reset mechanisms if available, which should incorporate secure authentication methods.

17.4.5 Multi-Factor Authentication (MFA)

MFA must be implemented for accessing sensitive systems and data, especially for remote access and administrative accounts.

MFA methods may include something the user knows (password), something the user has (security token or mobile app), or something the user is (biometric verification).

17.4.6 Roles and Responsibilities

- **Users:** Shall create and maintain passwords according to this policy, report any suspected password compromise, and participate in mandatory security training.
- **IT Support Companies:** Responsibilities for enforcing this policy, managing password-related incidents, and ensuring that password management systems are secure and compliant with policy requirements.
- **Management:** Must ensure that employees are aware of and comply with the password policy and provide support for policy enforcement.

17.5 Monitoring

The network operating system settings/restrictions make the monitoring of this policy mute.

17.6 Enforcement

This policy is enforced by the network operating system settings.

18 Artificial Intelligence (AI) Policy

18.1 Purpose

We are committed to using AI responsible and ethically within our organisation for both internal and customer purposes. This policy outlines our approach to AI governance adhere to the principles of ethics, ensuing compliance with standards, and safeguarding data privacy, integrity, confidentiality, transparency, and accountability. We are committed to continual improvement to using AI throughout our processes.

The purpose of this policy is to establish a structured approach for the use of AI within the company.

18.2 SCOPE

This policy applies to all employees, contractors, and third-party users of the organisation.

18.3 ETHICAL PRINCIPLES

- **Fairness**: Our AI systems are designed to avoid bias and discrimination. This means that we take proactive steps to ensure that our algorithms and data sources are fair and equitable.
- **Transparency**: We maintain clarity and openness in our algorithms, data sources, and decision-making processes. This transparency helps build trust with our stakeholders.
- **Accountability**: We define clear roles and responsibilities to ensure accountability in our AI practices. This includes having designated individuals or teams responsible for overseeing AI initiatives.
- **Data Privacy**: We protect data in accordance with relevant regulations, such as the Protection of Personal Information Act (POPI), and adhere to established information security standards.

18.4 AI DEVELOPMENT AND DEPLOYMENT

- **Data Quality:** We use high-quality data from our operations to maintain the accuracy and reliability of our AI systems. This involves rigorous data collection and validation processes.
- **Model Evaluation:** Before deploying AI models, we thoroughly test and validate them to ensure they meet our performance and security standards. This helps us identify and mitigate potential risks.
- **Human Oversight:** We ensure that human intervention is present in critical decisions made by AI systems. This human oversight ensures accountability and ethical considerations. It is essential to ensure that relevant regulations and requirements are considered and adhered to.
- **Continual Improvement:** We promote a culture of learning and improvement, encouraging our teams to adapt to new challenges and advancements in AI technology.
- **Information Security:** We protect the integrity, confidentiality, and availability of data used in our AI systems. This includes implementing robust security measures to safeguard against data breaches and other threats.
    - **Open-source AI** tools are powerful and innovative but often lack the necessary security to protect data, including user information. The risk of data breaches, unauthorized access, and misuse is a significant concern, consider this before using any data from the organisation.

18.4.1 STAKEHOLDER ENGAGEMENT

- **Customer Consultation**: We engage with our stakeholders to understand their needs and expectations regarding AI. This helps us tailor our AI solutions to better serve our customers.
- **Employee Training**: We provide regular training on ethical AI practices to our employees. This ensures that our teams are well-informed and equipped to handle AI responsibly.
- **External Collaboration**: We collaborate with external partners for knowledge sharing and to stay updated on the latest developments in AI. This collaboration helps us continuously improve our AI practices.

18.4.2 COMPLIANCE AND REPORTING

- **Regulatory Compliance**: We adhere to all relevant AI regulations and standards. This includes staying informed about changes in the regulatory landscape and adjusting our practices accordingly.
- **Internal Audits**: We conduct regular audits to ensure compliance with our AI governance policies. These audits help us identify areas for improvement and maintain high standards.
- **Transparency Reports:** We provide periodic reports to maintain transparency with our stakeholders. These reports detail our AI practices, performance, and any incidents or issues that have arisen.

- **Information Security:** We report any suspected information security incidents promptly and take appropriate actions to address them.

18.5 CONCLUSION

Our AI policy ensures that we deploy AI responsibly and engage with our stakeholders effectively in serving our customers, upholding integrity, confidentiality, availability, and privacy, we aim to build trust and deliver value to our customers. We are committed to continually improvement and adherence to international standards in all our AI initiatives.

19 INFORMATION INCIDENT REPORTING POLICY

19.1 PURPOSE

The purpose of this policy is to establish a structured approach for reporting and managing information security incidents to ensure compliance with ISO27001 standards and applicable regulations.

19.2 SCOPE

This policy applies to all employees, contractors, and third-party users of the organisation.

19.3 DEFINITIONS

- **Information Security Incident**: Any event that has the potential to compromise the confidentiality, integrity, or availability of information assets.
- **Incident Report**: A documented account of the information security incident.

19.4 INCIDENT REPORTING

- **Reporting Channels:** All information security incidents must be reported immediately to the chief digital officer, information security manager (ISM), IT support company/system administrator and information officer.
- **Reporting Procedure:**
    - Identify and document the incident.
    - Report the incident to your supervisor, ISM, IT support company/system administrator and information officer.
    - IT support company will follow their incident response plan for Schauenburg and provide details/outcomes to information officer, ISM and relevant team.
    - Provide all relevant details, including the nature of the incident, affected systems & information assets, and any immediate actions taken.

19.4.1 INCIDENT MANAGEMENT

- **Initial Assessment**: The ISM, with the IT support company, will conduct an initial assessment to determine the severity and impact of the incident.
- **Containment**: Immediate actions will be taken to contain the incident and prevent further damage.
- **Investigation**: A thorough investigation will be conducted to identify the root cause and extent of the incident.
- **Resolution**: Appropriate measures will be implemented to resolve the incident and restore normal operations.
- **Documentation**: All incidents will be documented, including the details of the incident, actions taken, and lessons learned.

19.4.2 COMMUNICATION

- **Internal Communication**: Relevant stakeholders will be informed about the incident and the actions being taken.
- **External Communication**: If necessary, external parties such as service providers, customers, partners, and regulatory authorities will be notified in accordance with legal and contractual obligations.

19.5 TRAINING AND AWARENESS

All employees will receive regular training on incident reporting procedures and their responsibilities in maintaining information security

19.6 ENFORCEMENT

- **Violations:** Non-compliance with this policy will result in disciplinary action, up to and including termination of employment.

20 ASSET DISPOSAL POLICY

20.1 PURPOSE

The purpose of this policy is to outline the procedures for the secure disposal of assets to protect sensitive information and ensure compliance with ISO 27001 standards.

20.2 SCOPE

This policy applies to all physical and digital assets owned by the organization, including but not limited to computers, servers, storage devices, mobile devices, and paper documents.

20.3 DEFINITIONS

Asset: Any resource or item of value owned by the organisation, includes hardware, firmware, software, practices, procedures, and data.

Disposal: The process of securely removing or destroying assets that are no longer needed or are being replaced.

Computer Decommission Form: Form that is required to be completed in connection with any disposal of an asset.

20.4 POLICY

20.4.1 ASSET IDENTIFICATION

All assets must be inventoried and tracked throughout their lifecycle. Before disposal, assets must be recorded in the asset register.

Assets must be classified based on the sensitive of the data they contain and their impact on the organisation it compromised.

20.4.2 DATA SANITISATION

All sensitive data must be removed from digital assets before disposal. This may include data wiping, degaussing, or physical destruction of storage media. This includes any software under license to organisation.

Data sanitisation methods must comply with recognized standards to ensure that data cannot be recovered.

20.4.3 PHYSICAL DESTRUCTION

For assets that cannot be effectively sanitised, physical destruction methods (shedding, crushing, …) must be reused to ensure that data cannot be reconstructed or retrieved.

Engage with certified disposal vendors to ensure that physical destruction meets industry standards and provides certificates of destruction when applicable.

20.4.4 DOCUMENTATION AND APPROVAL

Disposal requests must be submitted using the IT support company's "Computer Decommission Form" and approved by authorised personnel, including documentation of the asset's details and the reason for disposal.

Maintain records of all disposed assets, including the method of disposal, date of disposal, and authorisation documentation.

20.4.5 ENVIRONMENTAL CONSIDERATIONS

Ensure that asset disposal methods comply with environmental regulations and standards for recycling and waste management.

Where possible, assets should be recycled through certified approved and certified e-waste recycling programs.

20.4.6 THIRD PARTY DISPOSAL

When using a third-party vendor for asset disposal, they will firstly be vetted and meet security requirements. '

Establish contracts with the disposal vendors that includes clauses on data security, confidentiality, and compliance with relevant regulations.

20.4.7 SECURITY INCIDENTS

Any security incidents or breaches related to asset disposal must be reported immediately to the information security officer.

The organisation will investigate incidents and take corrective actions to mitigate any potential impacts.

20.5 ROLES AND RESPONSIBILITIES

- **Employees:** Must follow the asset disposal policy and ensure that assets are properly prepared for disposal according to this policy.
- **IT Support Company:** Responsibilities for overseeing data sanitization, coordination with disposal vendors, and maintaining records of disposal assets.
- **Management:** Must ensure that the disposal asset policy is implemented and that adequate resources are provided for its enforcement.

21 REFERENCE DOCUMENTS

Reference Document Number / Applicable Date	Document Title	Applicable Section
ISO27001	*Internation Standard for Information Security Management Systems*	
ISO42001	*International Standard for Artificial Intelligence Management Systems*	
POL-09924	*Information Security Policy*	
PRC-00003	*Documentation Management Procedure*	*7.4*
STD-09459	*Leadership*	
STD-09464	*Context of the organisation*	
STD-09465	*Operation*	
STD-09467	*Performance Evaluation*	
STD-09468	*Improvement*	
STD-09469	*Planning*	
STD-09470	*Support*	

22 DEFINITIONS

Listed are all the definitions of Terms used in this document

Term	Definition
Author	An author is the creator or originator of any written work such as a document or book and is thus also a writer. More broadly defined, an author is "the person who originated or gave existence to anything" and whose authorship determines responsibility for what was created.
Designated User	This is an individual person identified as a subject matter expert who has the experience to determine the information present is Clear, Concise and Valid to perform the Service function or produce the product defined in the document.
Process Owner	Business Individual who has the ultimate responsibility for the successful implementation (manually or through IT solutions), performance and continuous improvement of all levels of a specific process. The process owner is empowered and has the authority and ability to make decisions on necessary process changes.
Release Authority	This is a person has been given the responsibility to manage a Service or a Project within schedule and budget.
Business Domain	A collection of microcomputer systems configured as a Windows Active Directory Domain. Components include login account management and configuration policy implementation.
Windows Update	Managed by N-Central
Managed Configuration	Computer configuration autonomously controlled by N-Central.
Login account	A username and password given to company employees that is used specifically for company resources.
Account Holder	Any employee of the company with a login account.
Email Account	A company email address associated with login account, typically username@schauenburg.co.za or username@stratosat.co.za
Company	Schauenburg International – Africa Group that includes Schauenburg (Pty) Ltd, Schauenburg Systems (Pty) Ltd, Stratosat Datacom SA (Pty) Ltd and Stratosat West Africa Ltd
Organisation	Schauenburg International – Africa Group that includes Schauenburg (Pty) Ltd, Schauenburg Systems (Pty) Ltd, Stratosat Datacom SA (Pty) Ltd and Stratosat West Africa Ltd
IT Support Company	Company appointed service provider responsible to perform services and support as per agreements.
File Storage	A place where user data is stored. Typically, data on the login account's S: drive.
Supervisor	The individual responsible for supervision of the account holder.
System Administrator	The title is associated with the person responsible for core IT resources, such as email, file server, and network access.
CFO	Chief Financial Officer, manager for all IT resources, who is the interface between company employees and IT resources.
Information Security Officer	As per appointment letter and is the individual that manages for all IT resources, who is the interface between company employees and IT resources.

Data Restoration	The retrieval of files, folders, or email from archive media.
Email Storage	All items stored on the Company's email server
S: Drive	Shared file storage for all company employees to access.
R: Drive	Restricted storage for certain employees only
U: Drive	File storage allocated for individual account holders on the Company file server.
Domain Administrators	Members of a highly restricted security group that are tasked with being technically and directly responsible for certain IT assets at the Company.
Full Control	Ability to grant permissions to other account holders to the given folder, subfolder, or file. Typically reserved for Domain Administrators.
Subsidised computers	Computers that the employee/contractors purchase for themselves as they receive a computer allowance from the company

23 ABBREVIATIONS/ACRONYMS

Abbreviation / Acronyms	Description
CP	Change Proposal
HR	Human Resources
ISO	International Standards Organisation
IMS	Integrated Management System
R	Revision
T-N-R	Document Type, Unique Number, Revision Number
Com	Company
Dep't	Department
ISMS	Information Security Management System
IT	Information Technology
Organisation	Schauenburg (Pty) Ltd Schauenburg Systems (Pty) Ltd Stratosat Datacom SA (Pty) Ltd
AI	Artificial Intelligence