TRANSNET

Transnet Group

INFORMATION SECURITY POLICY

Policy Reference Number	*TG/EISM 8/4/3P*
Version Number	*3.0*
Effective Date	*March 2022*
Review Date	*March 2027*
Policy Owner	*GM: Cyber Security, Governance, Risk and Compliance*
Signature	Stephen Mark
Policy Sponsor	*Group Chief Information Officer*
Signature	
Date Approved	10/5/2022

Stakeholders

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Compulsory Stakeholder Involvement						
Subject Matter Experts	Daniel Ehrke	ICT Governance, Risk and Compliance Manager	Daniel Ehrke	Feb 10, 2022	Daniel.Ehrke@transnet.net	084 445 6799
Group Risk	Virginia Dunjwa	GM: Group Enterprise Risk	Virginia Dunjwa (Feb 11, 2022 11:12 GMT+2)	Feb 11, 2022	Virginia.Dunjwa@transnet.net	060 847 1114
Compliance	Kgomotso Modise	GM: Group Compliance	Modise	Feb 23, 2022	Kgomotso.Modise@transnet.net	083 444 0047
Group Legal Services	Sue Albertyn	GM: Labour Law & Consequence Management	Sue Albertyn Sue Albertyn (Feb 23, 2022 14:45 GMT+2)	Feb 23, 2022	Sue.Albertyn@transnet.net	011 308 3630
Transnet Internal Audit	Busiwe Quma	GM: Technology and Technical Assurance – Internal Audit	n/a	n/a	Busiwe.quma@transnet.net	011 308 4501
Organised labour via Employee relations management	Neo Bodibe	GM: Employee Relations	Neo Bodibe (Apr 21, 2022 15:43 GMT+2)	Apr 21, 2022	Neo.Bodibe@transnet.net	083 762 0185

Recommended by Policy Owner and Policy Sponsor:

I hereby acknowledge that a search has been conducted and that the Policy is not duplicated or in conflict with any other Transnet Policies.

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Policy Owner	Stephen Mark	GM: Group Cyber Security, Governance, Risk and Compliance	Stephen Mark	Feb 10, 2022	Stephen.Mark@transnet.net	072 474 5597
Policy Sponsor	Pandelani Munyai	Group Chief Information Officer		10/5/2022	Pandelani.Munyai@transnet.net	064 809 9622

Group Executive Committee

Final Approval

23 June 2022

Date Signed Off

Summary of Version Control

Version Number	Effective Date	Summary of Changes
1.0	*November 2011*	*First release of the Policy.*
1.2	*August 2014*	*General updates to the Policy.*
1.3	*November 2014*	*Update headers and footers and corrected index numbers.*
2	*October 2015*	*General updates to the Policy.*
3	*January 2022*	*Formatting updated; content aligned with the latest ISO27001 standard.*

Contents

1 BACKGROUND

1.1. Transnet business relies on Information and Communications Technology (ICT) to provide an environment where business operations are executed in a smooth, un-interrupted and secure manner, while maintaining the confidentiality of information, such as financial information and operational procedures. At the same time, the current regulatory and legal frameworks place significant emphasis on the Information and Communications Technology Governance and specifically in the protection of information.

1.2. The Information Security Policy defines the approach and outlines the requirements that the Information Technology management must fulfil in order to provide business with a secure Information and Communication Technology (ICT) operations environment. The ICT Security policy is aligned to the ICT Governance Policy and the relationship is shown in Figure 1.

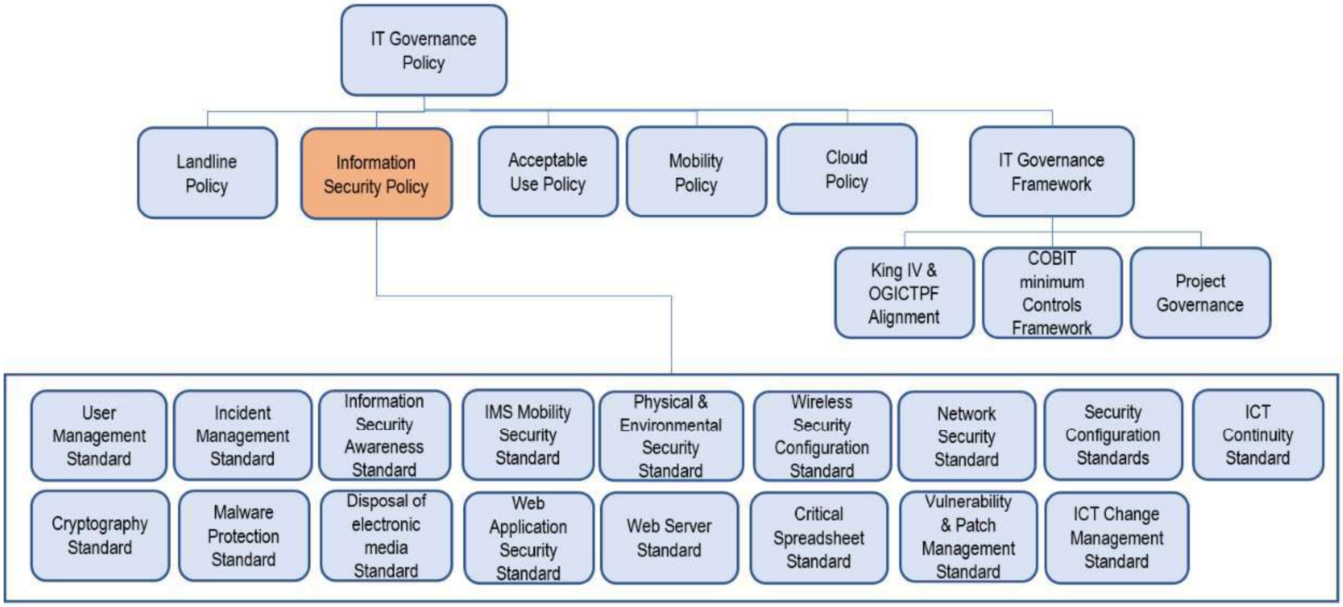
IT Governance Policy
Landline Policy
Information Security Policy
Acceptable Use Policy
Mobility Policy
Cloud Policy
IT Governance Framework
King IV & OGICTPF Alignment
COBIT minimum Controls Framework
Project Governance
User Management Standard
Incident Management Standard
Information Security Awareness Standard
IMS Mobility Security Standard
Physical & Environmental Security Standard
Wireless Security Configuration Standard
Network Security Standard
Security Configuration Standards
ICT Continuity Standard
Cryptography Standard
Malware Protection Standard
Disposal of electronic media Standard
Web Application Security Standard
Web Server Standard
Critical Spreadsheet Standard
Vulnerability & Patch Management Standard
ICT Change Management Standard

Figure 1

1.3. The Information Security Policy was developed and aligned to the ISO 27002 standard. The ISO 27002 standard is the code of practice for information security. It outlines potential controls and control mechanisms, which may be implemented.

1.4. The Information Security Policy establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management for the following areas (refer to figure 2):

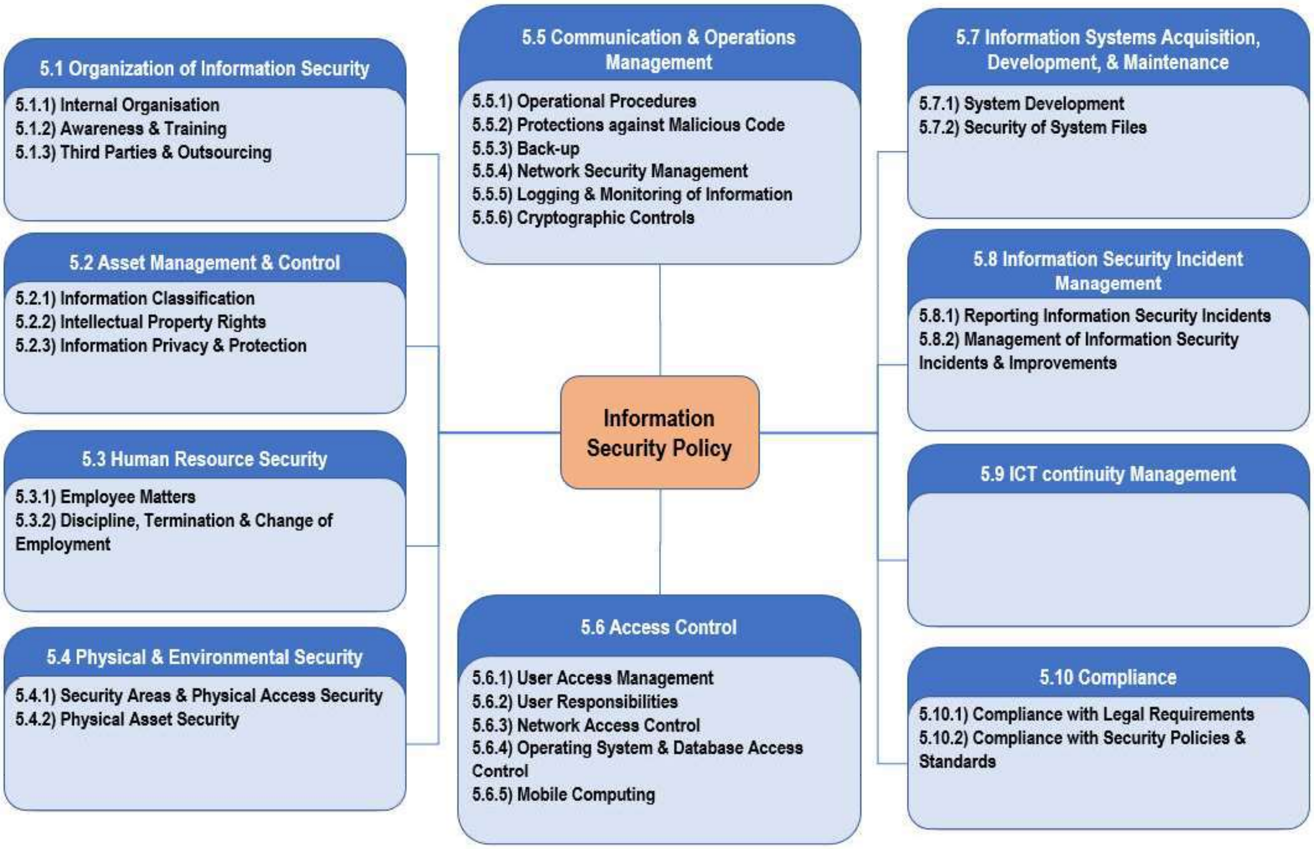
Information Security Policy
5.1 Organization of Information Security
5.1.1) Internal Organisation
5.1.2) Awareness & Training
5.1.3) Third Parties & Outsourcing
5.2 Asset Management & Control
5.2.1) Information Classification
5.2.2) Intellectual Property Rights
5.2.3) Information Privacy & Protection
5.3 Human Resource Security
5.3.1) Employee Matters
5.3.2) Discipline, Termination & Change of Employment
5.4 Physical & Environmental Security
5.4.1) Security Areas & Physical Access Security
5.4.2) Physical Asset Security
5.5 Communication & Operations Management
5.5.1) Operational Procedures
5.5.2) Protections against Malicious Code
5.5.3) Back-up
5.5.4) Network Security Management
5.5.5) Logging & Monitoring of Information
5.5.6) Cryptographic Controls
5.6 Access Control
5.6.1) User Access Management
5.6.2) User Responsibilities
5.6.3) Network Access Control
5.6.4) Operating System & Database Access Control
5.6.5) Mobile Computing
5.7 Information Systems Acquisition, Development, & Maintenance
5.7.1) System Development
5.7.2) Security of System Files
5.8 Information Security Incident Management
5.8.1) Reporting Information Security Incidents
5.8.2) Management of Information Security Incidents & Improvements
5.9 ICT continuity Management
5.10 Compliance
5.10.1) Compliance with Legal Requirements
5.10.2) Compliance with Security Policies & Standards

Figure 2 – Information Security Policy Areas

2 PURPOSE

2.1 The purpose of this policy is:

- Ensure compliance with current laws, and regulations,
- Ensure administrators and employees maintain the responsibility for ownership and knowledge about information security in order to minimise the risk of security incidents,
- Establish controls for protecting Transnet's information and information systems against abuse and other forms of harm or loss.

2.2 An Information Security policy statement expresses management's commitment to the implementation, maintenance, and improvement of its Information Security management system.

3 DEFINITIONS AND ABREVIATIONS

For ease of reference words, expressions and abbreviations used in the policy are defined below:

3.1 **Asset:** Any tangible or intangible object that has value to Transnet and includes, but is not limited to information, systems, facilities, networks, and computers.

3.2 **Business impact analysis (BIA):** The process by which the impact of a disaster or a business interruption on key business processes from both a quantitative and qualitative perspective are assessed, to include financial implications, performance impacts and any perceived impression on the brand or reputation of the organization. The BIA helps management decide for which business processes planning may be required and which continuity strategies to implement.

3.3 **Communication:** Includes both a direct communication and an indirect communication.

3.4 **Control:** Is any administrative, management, technical, or legal method that is used to manage risk. Controls are safeguards or countermeasures. Controls include practices, policies, procedures, programs, techniques, technologies, guidelines, and organisational structures. Controls can be deterrent, preventive, protective, detective, or corrective and typically are implemented to deal with a variety of root causes which result in risk.

3.5 **Cryptographic controls:** These are measures employed in the protection of information against unauthorised or unintentional disclosure and/or unauthorised alteration of the information.

3.6 **Demilitarised Zone:** Demilitarised zone is a sub-network (physical or logical) that contains a company's external services to a non-trusted network, such as the Internet.

3.7 **Direct communication:**

- Oral communication other than an indirect communication between two or more persons which occurs in the immediate presence of all the persons participating in that communication, or
- Utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who at the time that the indirect communication occurs is in the immediate presence of the person participating in the indirect communication.

3.8 **Employees:** means anyone who is on an indefinite contract of employment or on a fixed term contract or any person who works for Transnet, and who receives, or is entitled to receive remuneration, and any other person who in any manner assists in carrying on or conducting the business of Transnet, excluding independent contractors.

3.9 **Encryption:** Is the process of transforming readable information into something unreadable using an algorithm (or cipher) and a cryptographic key. The input into the process is often referred to as the plaintext and the output is known as the ciphertext.

3.10 **Entity:** Includes both individuals and processes.

3.11 **ICT:** Information and Communications Technology is the integration of telecommunications, computers, software, storage and systems that enable users to manipulate, transmit, access, and store information.

3.12 **ICT Continuity:** Capability of the organization to plan for and respond to incidents and disruptions in order to continue ICT services at an acceptable predefined level.

3.13 **ICT Continuity Plan/ Disaster Recovery Plan:** A written plan used to respond to the disruption of an organization's operations. This plan may focus on response to specific disruption scenarios.

3.14 **ICT Risk:** business risk associated with the use, ownership, operation, involvement, influence, and adoption of ICT within Transnet. It consists of ICT related events that could potentially impact the business considering both the likelihood and the impact of occurrence. It can occur with uncertain frequency and magnitude and it creates challenges in meeting strategic goals and objectives.

3.15 **IMEI:** International Mobile Equipment Identity, is a unique identification number assigned to identify devices with a sim card slot like mobile phones, tablets, or laptops. GSM networks use the IMEI number to identify and stop stolen devices from accessing the network.

3.16 **Indirect communication:** The transfer of information, including a message or any part of a message, whether:

- In the form of speech, music or other sounds, information, text, visual images (whether animated or not), signals or radio frequency spectrum, or
- In another form or in any combination of forms that is transmitted in whole or in part by means of a postal service or a telecommunication system.

3.17 **Information Asset:** Is information that has value to the extent that it enables Transnet to achieve business goals.

3.18 **Information:** The quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

3.19 **Information processing facility:** Any system, service, infrastructure, and the physical locations that house these.

3.20 **Information Resource:** The information and information assets of an organisation, department, or unit.

3.21 **Information Security events:** Indicates that the security of an information system, service, or network may have been breached or compromised. An Information Security event indicates that an Information Security policy may have been violated or a safeguard may have failed. This is a single event.

3.22 **Information Security incident:** Is made up of one or more unwanted or unexpected Information Security events that could potentially compromise the security of your information and weaken or impair your business operations.

3.23 **Information Security Management System (ISMS):** An Information Security Management System (ISMS) includes all of the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve information. It includes all of the elements that organisations use to manage and control their Information Security risks. An ISMS is part of a larger management system.

3.24 **Information Security:** aims to achieve, maintain, and regulate appropriate levels of:

- **Confidentiality:** Ensuring that information is accessible only to those authorised to have access to the information and to ensure that it is not made available or disclosed to unauthorised entities,
- **Integrity:** Safeguarding the accuracy, unauthorised alteration and completeness of information and processing methods,
- **Availability:** Ensuring that authorised users have access to information and associated assets when required.

3.25 **Information System:** Is a system for generating, sending, receiving, storing, displaying, or otherwise processing information messages and includes the internet.

3.26 **Interception:** Means the aural or other acquisition of the contents of any communication through any means, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication and includes the:

- Monitoring of any such communication by means of a monitoring or interception device,
- Viewing, examination or inspection of the contents of any indirect communications,
- Diversion of any indirect communication from its intended destination to any other destination.

3.27 **ISGRC:** Information Security, Governance, Risk and Compliance.

3.28 **Keystroke Monitor:** A specialised form of interception software or hardware, that records every key stroke by a user and, possibly, every character of the response that returns to the user.

3.29 **Malicious Code:** Code, the execution of which may result in the loss of the integrity, confidentiality, or availability of information. Examples include, but are not limited to viruses, worms and trojan horses.

3.30 **Minimum Control Framework (MCF):** Is a selected subset of controls from the COBIT framework selected by EIMS in consultation with TIA.

3.31 **Mobile Code:** Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction. Mobile code is associated with a number of middleware services.

3.32 **Mobile computing device administrator:** The appointed administrator/champion to manage mobile computing devices assigned to users.

3.33 **Mobile Devices or Mobile Computing and Storage Devices:** A portable device that allows people to work with information either locally or through a network connection. This includes, but is not limited to, notebooks, laptops, tablets, PDAs and smart phones. The definition excludes single purpose devices, such as hand-held terminals.

3.34 **Monitoring:** The method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of: user account logs, application logs, information backup and recovery logs, automated intrusion detection system logs, etc.

3.35 **Network Devices:** Network devices are components used to connect computers or other electronic devices together so that or that share files or resources such as printers

3.36 **Owner (Asset, Information, Information, Application):** Owners are formally responsible for making sure that assets / information / information / applications are secure while they are being developed, produced, maintained, and used.

3.37 **Platform:** A system on which application programs can run. Mobile phones running iOS, Symbian and Android are examples of platforms.

3.38 **Recovery Point Objective (RPO):** The recovery point objective of a set of information is the point in time to which the information must be restored for acceptable use of a system e.g. three days ago.

3.39 **Recovery Time Objective (RTO):** The timeframe that is available for the restoration of processes or service areas. Going beyond the RTO is the point at which a business is no longer viable.

3.40 **RICA:** The Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002.

3.41 **Sensitive Information:** Information which is currently not in the public domain. This information should be protected against unauthorised access or unwarranted disclosure. This would include the personal information of employees and commercially sensitive information.

3.42 **System Files:** System files refer to Operating System, database and application files that are important for the operation of an Operating System, database or application.

3.43 **Third party:** In the context of a specific issue, a third party is any person or body that is recognised as independent of the people directly involved with the application and implementation of this policy.

3.44 **Threat:** A threat is a potential unwanted event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organisation or system.

3.45 **TIA:** Transnet Internal Audit.

3.46 Transnet or “The Company” or “The Group”: Transnet SOC Ltd.

3.47 **Vulnerability:** Vulnerability is a weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harmed by one or more threats.

4 SCOPE

4.1 Information Security Policy covers the provision of organisational, technical and social measures necessary to safeguard information assets against unauthorised access, disclosure, denial of use, modification, diversion, destruction, loss, theft, or misuse, both malicious and accidental. The Information Security Policy jurisdiction covers all Transnet information assets (located at Transnet and non-Transnet locations) and begins with the electronic input of information and ends with its output using an electronic or non-electronic output medium.

4.2 The Information Security Policy applies to the Transnet Group and all Operating Divisions, including third parties servicing Transnet, employees, service providers and consultants.

5 POLICY STATEMENTS

5.1 ORGANISATION OF INFORMATION SECURITY

Internal Organisation

5.1.1.1 The Information Security Human Resources structure with detailed roles and responsibilities must be defined by the Information Security senior management.

Awareness and Training

5.1.1.2 An information awareness programme to promote compliance with information security regulations, policies and standards and promote protection of Transnet information assets, must be conducted by the Transnet ISGRC team annually.

Third Parties and Outsourcing

5.1.1.3 Third party access to Transnet information assets must be based on a formally executed contract. This contract must stipulate that all employees or agents of the third party are required to comply with all appropriate Transnet Information Security policy statements.

5.1.1.4 Prior to signing any ICT support agreement with a third party, the following requirements must be respected, and if necessary, included in the third-party contract:

- The definition of security administration, management, and control objectives,
- The separation of Transnet's and the third party's information, if on an external system the restrictions on copying information and securing assets,
- The right of Transnet to intercept Transnet communications must be in accordance with POPIA and RICA requirements,
- The requirement to prohibit access to Transnet information and systems without explicit authorisation from Transnet. and to maintain a list of individuals who have access to such information or system,
- The right of Transnet to monitor (and revoke) administrator rights,
- Facilities to rapidly disable any individual user ID,
- The responsibilities and procedures for reporting and handling security incidents,
- The right of Transnet to audit contractual responsibilities,
- The right of Transnet to perform on-site inspections of the information centre of external third parties.

5.1.1.5 The third party must ensure that all its employees and agents who have access to Transnet information are aware of and carry out their security responsibilities with respect to that information.

5.1.1.6 Third party access to Transnet information assets must be set to "no access" by default (i.e. all access rights must be explicitly granted). When granted, third party access to Transnet information assets must be for the minimum necessary period of time. Access to the assets must be approved by the asset owner(s) and the information process owner (if different from owner) or the GM: Cyber Security, Governance, Risk and Compliance.

5.1.1.7 Third party remote access to Transnet information assets will only be authorised in cases where there is a clearly defined business need. The access facility provided must limit the third party to the agreed method of access, the agreed access rights, and the agreed level of functionality.

5.1.1.8 Third party remote access to Transnet information assets must be approved by the asset owner(s) and the information process owner (if different from owner) or the Group CIO or GM: Cyber Security.

5.1.1.9 A regular review of all previously approved third party remote access must be conducted by the information owner. Any changes to the conditions upon which the third-party access was previously granted must be reviewed.

5.1.1.10 Prior to the implementation of a third-party remote access, the implementing party must request that an Information Security risk assessment be conducted by ISGRC and approved by the GM: Cyber Security, Governance, Risk and Compliance. to determine the necessary level of controls for that connection. All third-party connections must be classified according to the type of access required for the connection, thereby identifying the necessary security controls required for the connection approval.

5.1.1.11 When third party access needs to be granted with system-level privileges (e.g. root or supervisor level access), such rights must be granted for a limited duration, and de-activated when not required. The access usage must be subject to supervision and must be fully logged.

5.1.1.12 The third party must comply with all Transnet Information Security policies, standards and procedures. information assets that have been entrusted to a third party must only be used by the third party for the purposes agreed. Transnet information must not be disclosed to any non-Transnet party for any purpose other than the one that has been expressly authorised by Transnet.

5.1.1.13 Third party access to Transnet information assets, and in particular, access to customer information must be in accordance with legal and regulatory requirements for trade and business secrecy and information protection.

5.1.1.14 A risk assessment must be carried out by the ISGRC team and approved by the GM: Cyber Security before considering the outsourcing of an information service.

5.1.1.15 Third party contracts must include controls for the protection of sensitive information.

5.1.1.16 Local laws must always be considered prior to outsourcing services or storing information in cross border locations. Unless the local laws at the outsourcing location can guarantee adequate protection of the information, outsourcing cross national borders is not permitted.

5.1.1.17 Contracts must always give Transnet the right to audit the service provider to ensure compliance with the contractual requirements.

5.2 ASSET MANAGEMENT AND CONTROL

Information Classification

5.2.1.1 Information must be classified in terms of its value, legal requirements, sensitivity and criticality to the organisation in accordance with Transnet's Information Classification Policy. The minimum requirement for protecting the confidentiality of all information regardless of classification is the application of access control and authorisation.

5.2.1.2 All information removed from the Transnet premises, for offsite backup reasons or the repair of hardware devices (PC's, servers), must be adequately secured and controlled before the release of the information from the premises.

5.2.1.3 All sensitive information must be properly deleted from the media, including backups, with no residue remaining that could be recovered by unauthorised individuals.

Intellectual Property Rights

5.2.1.4 Without specific written exceptions, all programs and documentation generated by personnel for the benefit of Transnet are the property of Transnet. All computer programs and documentation owned by Transnet must include appropriate copyright notices.

5.2.1.5 All software on Transnet computers is protected by copyright laws. Commercial software purchased by Transnet is authorised for Transnet use only and must be utilised in accordance with contractual agreements and copyright laws. Unless specifically authorised within the license agreement, making copies of copyrighted software for personal use is prohibited.

5.2.1.6 Transnet strongly supports strict adherence to software vendor license agreements and copyright holder notices. Whenever bundled systems are being procured, the source must provide written evidence of the software licenses. The agreements for all computer programs licensed from third parties must be periodically reviewed for compliance and additional licensed copies procured as required.

5.2.1.7 Transnet critical hardware and software products must be registered with the appropriate vendors to assure that support and upgrades are readily available.

5.2.1.8 Transnet information, computer software and other information assets must be used for authorised business purposes.

Information Privacy and Protection

5.2.1.9 Transnet employees must ensure that personal information stored in Transnet devices is secured and protected. Transnet makes all reasonable efforts to respect the privacy of information stored on Transnet information assets.

5.2.1.10 Transnet reserves the right to have authorised personnel intercept information at the user level or user communications in the best interests of Transnet or in contravention of Transnet policies. This will be conducted in compliance with requirements specified by POPIA and RICA.

5.3 HUMAN RESOURCES SECURITY

Employee Matters

5.3.1.1 Transnet employees, contractors and third-party users / vendors must act in accordance with Transnet's Information Security Policy and accompanying standards, guidelines and procedures.

5.3.1.2 Individuals in the possession of portable laptops, notebooks, smartphones, tablets, and other transportable computers or storage media (such as USB devices) containing Transnet information must not leave these unattended at any time unless the device and information has been properly safeguarded. Such individuals take full responsibility for the equipment and the information it retains.

Discipline, Termination and Change of Employment

5.3.1.3 In all cases, where employees terminate their employment with Transnet, they must return all Transnet equipment and information back to Transnet.

5.3.1.4 Upon the termination or expiration of their contract, all contractors, consultants, and temporary staff must relinquish all copies of Transnet information received or created during the performance of the contract.

5.3.1.5 The access rights of the above parties to Transnet information and information processing facilities must be removed upon termination of their employment, contract or agreement.

5.4 PHYSICAL AND ENVIRONMENTAL SECURITY

Secure Areas and Physical Access Security

5.4.1.1 Buildings that house Transnet computers or communications systems must be protected with physical security measures that prevent unauthorised persons from gaining access.

5.4.1.2 To ensure that only authorised personnel are allowed access, security perimeters such as walls, card controlled entry gates or manned reception desks must be used to protect areas that contain information and information processing facilities.

5.4.1.3 Printers used for printing confidential information must not be left unattended if they are located in an open environment. Secure printing must be used whenever supported by a printer. Printed material must be appropriately handled and protected by the person that printed them.

5.4.1.4 Access to Transnet information equipment by hardware maintenance staff must be controlled. This includes proper staff identification, logging of work done, and supervision to ensure that no unauthorised modifications are performed on any equipment other than that which is to be maintained.

Physical Asset Security

5.4.1.5 Transnet premises for information equipment must meet minimum environmental standards for power, cooling, humidity, etc. as per supplier recommendations to ensure continued availability and integrity.

5.4.1.6 The security requirements for equipment stored off-site must be the same as the requirements for on-site equipment.

5.4.1.7 Network control devices, diagnostic equipment, security firewall systems and encryption key management systems must be stored in physically secure locations.

5.4.1.8 All storage media must be disposed of as per the "Disposal of electronic Storage Media Standard".

5.4.1.9 During extended periods away from your desk, sensitive working documents must be placed in a securely locked area such as a locked drawer.

5.4.1.10 Employees must place all office documents in securely locked desks or cabinets at the end of the day.

5.4.1.11 Theft or loss of a Transnet asset must be reported to the Security department for investigation. The Security department is responsible managing access to Transnet physical facilities.

5.4.1.12 The owner or official user of the asset lost must report the incident to the South African Police Services (SAPS) and where applicable, the relevant service providers.

5.5 COMMUNICATIONS AND OPERATIONS MANAGEMENT

Operational Procedures

5.5.1.1 The following operational procedures exist as a minimum for all systems:

5.5.1.1.1 Logical access must be managed in a standardised manner in accordance with the requirements outlined in the "User Management Standard".

5.5.1.1.2 Operating procedures must be documented, maintained and available for information technology processes as necessary.

Protection against Malicious Code

5.5.1.2 Detection, prevention and recovery controls must be implemented to protect the Transnet Information Technology resources against malicious code.

Back-up

5.5.1.3 Backups must be performed as per documented schedules, monitored and stored off-site in secured locations.

5.5.1.4 Back-up copies of information and software must be protected at the same levels of security as the original information. Back-up copies of information and software must be restored for testing purposes on a periodic basis.

5.5.1.5 Backups of business information must be done on the business servers not on desktops.

Network Security Management

5.5.1.6 Network devices must be secured, managed and monitored by senior management to protect the devices and the information transmitted through them.

Logging and Monitoring of information

5.5.1.7 Auditing must be enabled on all systems at all times in accordance with the Minimum Control Framework.

5.5.1.8 Additional audit logs must be enabled to accommodate business or security requirements as per the application / information owner request and in accordance with the classification level of the information.

5.5.1.9 Audit logs must have the capability to be reviewed for identification of exceptions and are kept for a defined period of time in support of the review cycles.

5.5.1.10 Controls must be in place to protect the logging facilities and the information logged against tampering and unauthorised access.

5.5.1.11 The clocks of all the Transnet information processing systems must be synchronised with a NTP time source to ensure consistent time stamping of logs.

5.5.1.12 All technologies implemented in the Transnet environment must have a Minimum Security Baseline Standard.

Cryptographic Controls

5.5.1.13 Information must be encrypted in storage and in transit as per the requirements outlined in the "Information Classification Policy" for the respective level of classification.

5.6 ACCESS CONTROL

User Access Management

5.6.1.1 Access to applications, systems and resources must be granted in accordance with the relevant authorised job description profile.

5.6.1.2 User accounts and assigned privileges must be regularly reviewed by the information asset owner to ensure the validity of the user accounts, the segregation of duties and the appropriateness of the privileges assigned to the users.

User Responsibilities

5.6.1.3 Users must be reminded of their responsibility to comply with security policies and standards when they request or change access by submitting an Access Form.

5.6.1.4 Employees must not be allowed to intercept any information without authority or permission as doing so is an offence and may be prosecuted as per RICA.

Network Access Control

5.6.1.5 The capability of users to connect to the network and use network services must be restricted according to the job description profile of each user.

5.6.1.6 Ports services and similar facilities installed on a computer or network resources must be disabled or removed unless required for business purposes.

Operating System and Database Access Control

5.6.1.7 Access to the operating systems and databases must be configured securely. Logical access controls must be implemented to allow appropriate identification and authentication of users in order to limit the access exposure of the resources and the information stored in or processed by them.

5.6.1.8 Logical access management controls, including account and password controls must be implemented as per the "User Management Standard".

Mobile computing

5.6.1.9 Controls must be implemented to ensure the secure access to information on devices used for mobile computing. Such devices include smartphones, laptops, notebooks, and other portable computers. Users may bring their own devices into the Transnet environment subject to complying with all the security requirements applicable to Transnet owned equipment.

5.7 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

System Development

5.7.1.1 Information Security must be considered at all stages of the system development life cycle.

5.7.1.2 Transnet information systems must comply with all relevant Information Security policies, directives, standards, procedures and legal documents consistent with the business needs of Transnet.

5.7.1.3 A Transnet approved risk assessment methodology must be used to help ensure that appropriate Information Security controls are designed and built into new systems from the beginning.

5.7.1.4 Security mechanisms must be made available as modules that are technically separated from applications and that conform to internationally accepted standards wherever possible.

5.7.1.5 The technical and organisational binding of security services into applications must be based on standardised interfaces and processes.

5.7.1.6 Development staff must document all aspects of how Information Security has been considered and implemented at all stages of the software development life cycle (SDLC). When first published, such documentation must be issued to and approved by the Information Risk Security Governance and Compliance Steering Committee.

5.7.1.7 Developers must be responsible for the design and implementation of tests to ensure that Information Security controls meet previously specified acceptance criteria. The tests must be completed prior to production implementation.

5.7.1.8 The use of production information for development testing is prohibited. Information used for testing must be desensitised and approved by the information owner prior to release, use of desensitised production information must never jeopardise security or business-related privacy.

5.7.1.9 Business application systems must go into production when all users and information operations staff have received appropriate documentation and training in such issues as: how security incidents are handled, how emergency support access for developers is managed, and what users must do if they forget their password.

5.7.1.10 The ISGRC Steering Committee must confirm their approval that a new system satisfies all necessary security requirements prior to that system being used in a Transnet production environment.

5.7.1.11 Prior to moving software and/or system to production status, all special access paths must be removed so that access may only be obtained via normal secured channels.

5.7.1.12 The development environment must be physically or logically separate from the production environment. The development staff must not have access to production systems. The development staff may be granted access where appropriate lo their function for a limited period of time for essential support purposes.

5.7.1.13 All third party developed products used within Transnet must comply with Information Security policies, procedures, standards, etc. The installing agency must verify this compliance before the third party product is installed in Transnet.

5.7.1.14 A third party software product must be able to be integrated with the existing security system(s). of blocking unauthorised access to programs, functions, and information.

5.7.1.15 Standard procedures must be followed both for the tests and for the introduction of the third party software product into production.

5.7.1.16 System and information owners must be allocated prior to the implementation and go-live of a system.

5.7.1.17 Access to source code must be restricted to the relevant developers on the development environment and only production applications are installed on the production systems.

Security of System Files

5.7.1.18 Access to system or application sensitive files must be restricted to appropriate system users and is in accordance with the user's job function.

5.8 INFORMATION SECURITY INCIDENT MANAGEMENT

Reporting Information Security incidents

5.8.1.1 All employees, contractors and third party users of information systems and services must report security incidents to the Transnet Helpdesk.

Management of Information Security Incidents and Improvements

5.8.1.2 Reports of the incidents from the Helpdesk must be made available to the Information Risk Security Governance and Compliance Steering Committee (ISGRC-SSC) and must be used to identify trends or recurring incidents.

5.9 ICT CONTINUITY MANAGEMENT

5.9.1 ICT Continuity management must be a collaborative effort of the OD Heads of ICT and the Group CIO.

5.9.2 An ICT Continuity Programme must be developed and implemented for all Operating Division functions and EIMS functions to maintain essential customer services and critical business processes.

5.9.3 The ICT Continuity Programme must align with the Transnet Business Continuity management policy.

5.9.4 ICT continuity strategies must be developed based on the results of a formal a business impact assessment (BIA}.

5.9.5 ICT risk assessments (RA) must be conducted in line with the Transnet ICT Risk Management Framework including the continuity risks in the ICT Risk Universe.

5.9.6 The ICT continuity, processes standards and guidelines. must be reviewed, tested and updated every two years or after significant changes in order to verify that continuity objectives are achievable.

5.9.7 The ICT continuity plans. procedures and arrangements must be reviewed, tested and updated bi-annually or after significant changes in order to verify that continuity objectives are achievable.

5.9.8 An ICT continuity education programme must be established and maintained to ensure that all Transnet IMS employees that are responsible for ICT continuity are adequately and continuously trained. The training must enable the IMS employees to perform their required tasks competently.

5.9.9 An ICT continuity awareness programme must be established and maintained to ensure that ICT enabled Transnet employees are aware of ICT continuity arrangements and their roles, and responsibilities within the programme.

5.10 COMPLIANCE

Compliance with Legal Requirements

5.10.1.1 The developers of Information Security policies and standards must compile or update the respective documentation in-line with the legal and regulatory requirements outlined in the "Transnet Regulatory Universe". The regulatory requirements that affect Information Security are listed in section "Related Information and Reference" of the current document.

Compliance with Security Policies and Standards

5.10.1.2 Controls must be implemented to ensure compliance with the requirements set in the Information Security Policy and the supporting Standards. The controls must be documented and operated effectively and must cater adequately for deviations from technical standards in a manner which does not introduce risk to the business.

6 ROLES AND RESPONSIBILITIES

6.1 GM: ISGRC (CYBER SECURITY, GOVERNANCE, RISK AND COMPLIANCE)

6.1.1 Ensure security assessments of Information Security platforms are performed prior to those being approved. The platforms must conform to the Transnet security requirements.

6.1.2 Ensure that security configuration standards are defined and implemented for all platforms used to access or store Transnet information.

6.2 GROUP ISGRC STEERING COMMITTEE

The members of the committee must:

6.2.1 Participate in the development and maintenance of the Transnet Information Security Policy and the supporting standards,

6.2.2 Facilitate the deployment of the Transnet Information Security Policy to all Operating Division,

6.2.3 Monitor that all Operating Division ICT Departments complies with the Policy and report non-compliance.

Information Security Policy RACI

6.2.3.1 **Accountable:** Group Chief Information Officer and Senior Management.
6.2.3.2 **Responsible**: GM: Cyber Security, Governance, Risk and Compliance.
6.2.3.3 **Informed:** Operating Division's CIO.
6.2.3.4 **Support:** Group ICT.
6.2.3.5 **Monitoring and maintenance:** Information Security.

7 RELATED INFORMATION AND REFERENCE

This policy should be read in conjunction with the following documents, Policies and regulatory requirements:

7.1 INTERNAL DOCUMENTS:

7.1.1 Transnet Acceptable Use Policy,
7.1.2 Transnet Disposal of Electronic Storage Media Standard,
7.1.3 Transnet User Management Standard,
7.1.4 Transnet Register of Approved Mobile Platforms,
7.1.5 Transnet Cellular Procedures Document,
7.1.6 Transnet Records Management Policy,
7.1.7 Transnet Information Classification Policy,
7.1.8 Transnet Information Classification Standard,
7.1.9 Transnet Physical Environmental Standard,
7.1.10 Transnet Security configuration Standards,
7.1.11 Transnet Regulatory Universe,
7.1.12 Transnet Disciplinary Code and Procedures Policy.

7.2 EXTERNAL DOCUMENTS:

7.2.1 Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002) (RICA),
7.2.2 The Protection of Personal Information Act, 2013 (Act No 4 of 2013),
7.2.3 Electronic Communications and Transactions Act (Act No. 25 of 2002),
7.2.4 ISO 27001/2 (Information Security Management System and controls),
7.2.5 ISO 27031 (Guidelines for information and communications technology readiness for Business Continuity),
7.2.6 Copyright Act No 98 of 1978,
7.2.7 Intellectual Property Laws Rationalisation Act No.107 of 1996,
7.2.8 Promotion of Access to Information (Act 2 of 2000),
7.2.9 King IV Code on Corporate Governance,
7.2.10 Cybercrimes Act (Act no. 19 of 2020).

8 FINANCIAL IMPLICATIONS

8.1 Budget provision for the implementation of the policy should be allocated according to the cost centre management procedures.

9 EXCLUSIONS

9.1 There are no exclusions to this Policy.

10 REQUEST TO DEVIATE FROM POLICY

10.1 In cases where material and compelling circumstances merit deviation(s) from particular provision(s) of this policy, written submissions shall be submitted to the Group Cyber Security GM, who shall have full authority to grant such request, in whole or in part, or to refuse same.

10.2 Exceptions will only be allowed following a risk assessment and a signed risk acceptance from the Line Manager of the user. Thereafter, a waiver will be issued by the GM: Cyber Security, Governance, Risk and Compliance.

10.3 The exception will be granted for a maximum of six months and will have to be reviewed every six months if it is still required.

11 NON-COMPLIANCE

11.1 Breaches of this policy will be viewed in a very serious light. Employees who do not conform to this Policy or Principles and Standards may be subject to disciplinary action in terms of the applicable Transnet disciplinary processes and procedures.

11.2 Each Operation Division is responsible for ensuring compliance to the principles/rules of this Policy.