Information Security Policy

CGICT_ICT_001

Version 1.3

Version Control and Approval			
Document Name	Information Security Policy		
Document Number/Version	1.3.		
Status/Revision History			
Rev #	**Revision Update**	**Revised By**	**Date**
1.0	**New**	Author: William Nkuna	April 2017
1.1	Revision	Author: William Nkuna	September 2019
1.2	Revision	Author: William Nkuna	November 2019
1.3	Revision	Author: Mpumelelo Khumalo Ebrahim Mayet	June 2021
Approval			
Date Approved			
Date Last Amended	June 2021		
Date of Next Review	2023/24		
Related Policies	Information Security Policy, ICT Governance Framework, ICT User Account Management Policy		
Authored By			
Name	Mr. Mpumelelo Khumalo		
Position	Acting ICT Manager		
Signature		Date: June 2021	
Reviewed and Recommended by			
Name	Ms. Sibongile Ngwenya		
Position	Executive Manager: Corporate Services		
Signature		Date:	
Name	Mr. Thamsanqa Mdontswa		
Position	Chief Executive Officer		
Signature		Date: 30/03/2022	
Approved By			

Name	Ms. Portia Mushwana
Position	Chairperson: ICT Steering Committee
Signature	Date 30/03/2022

Approved By	
Name	Mr Chris Mudau
Position	Chairperson: Board and Accounting Authority
Signature	Date: 30/03/2022

Table of Contents

1 Introduction

The Safety and Security Sector Education and Training Authority (SASSETA) is dependent on information, Information systems and networks to ensure that the organisation delivers on its mandate. This information is therefore a critical resource in ensuring that the business objectives of the organisation are met. However, the information generated and the systems used to generate such information are subjected to accidental, criminal, malicious and natural threats that could potentially cause financial losses, disruption to business operations, loss of goodwill and disrepute to public image.

Information Security is the process of securing and protecting the organisation's information and data from unauthorised access, disclosure, modification, distribution or deletion. The SASSETA Information and Cyber Security Management System is achieved by implementing a set of controls which are not limited to policies, procedures and standards as well as technological and software applications. These controls assist in the rapid changing technology environment and mitigate and minimise the risks relating to the security of information and data of SASSETA. The Information Security requirements in this document is therefore essential to the safeguarding of the SASSETA assets (with particular references to data, information and information systems) and should be adhered to throughout SASSETA.

2 Definitions and Terms

Term/Acronym	Definition
Access Control	The controls management designed and implemented to enhance the control environment, by limiting access to data, information or computers and related devices.
Availability	Availability is the guarantee of reliable and constant access to data and information systems when required.
Confidentiality	The process followed to prevent unauthorised disclosure of information.
Information Technology Resources	The computer equipment, infrastructure, data, cloud services and information including the software.
Integrity	Integrity assures that the data or information system can be trusted. Ensures that it is edited by only authorised persons and remains in its original state when at rest.
Line Manager	The head of a business unit of SASSETA.
Restore	The process of recovering of data due to accidental data loss, disasters or due to data that is inaccessible.
System Administrator	An appointed SASSETA staff member who is appointed to create, amend, reset or delete system user profiles.
SLA	Service Level Agreement
User	Any person defined as an employee, sub-contractor, vendor support staff or temporary staff who has permission granted by the SASSETA

	management to access the Software application or SASSETA networks.

3 Legislative and Policy framework

3.1 Legislation

The South African laws and legislation that underpin this policy include the following:

- The Constitution of the Republic of South Africa, 1996 (Act 106 of 1996)
- Promotion of Access to information Act, 200 (Act 2 of 2000)
- Protection of Information Act, 1982 (Act 84 of 1982)
- Protection of Personal Information Act, 2013 (Act 4 of 2013)
- Electronic Communications and Transaction Act, 2002 (Act 25 of 2002)
- Regulation of Interception of Communication and Provision of Communication Related Information Act, 2002 (Act 70 of 2002)
- Copyright Act, 1978 (Act 98 of 1978)
- Archives and Records Service of South Africa Act, 1996 (Act 43 of 1996)
- Occupational Health and Safety Act, 1993 (Act 85 of 1993)
- Public Finance Management Act, 1999 (Act 1 of 1999 as amended by Act 29 of 1999)
- Public Service Act 1994, (Act 103 of 1994 as Proclaimed)
- National Strategic Intelligence Act, 1994 (Act 39 of 1994)

3.2 Applicable policies, standards and frameworks

The policy is developed taking into consideration the following standards and policy frameworks where relevant:

- ITIL
- KING 4 Report, Technology and Information Governance
- CoBIT 2019 Information Security Standards
- ISO Standards (17799, 27001 series and 38500)
- Minimum Information Security Standards (MISS)
- Minimum Physical Security Standards
- DPSA Corporate Governance of ICT Policy Framework (CGICTPF)
- National Cyber Security Policy framework 2012
- Electronic and Communications Transaction ECT Act 25 of 2002

4 The Purpose

The Purpose of this Policy is to ensure that a comprehensive approach is formulated to protect SASSETA's data, information and information systems against threats and vulnerabilities. The resources to be protected include but are not limited to networks, servers, computers, software, cloud services, removable media and data stored on all the devices and communicated through the resources. The ultimate aim is to protect all the resources against cyber-attacks, sabotage, unauthorised access, intrusions, malicious misuse and damage and inadvertent compromise.

5 Scope

This policy applies to all employees of SASSETA, contractors, third party service providers, partners, interns and temporary staff who store, utilise (process) and access the computer equipment, network infrastructure, data and all information systems applicable to SASSETA.

It also applies to all persons who directly or indirectly utilises and access the information and data that belongs to SASSETA whether kept within the premises or outside premises, cloud services, web based applications or hosted environments.

6 Policy Statement

The Information Security Policy establishes standards, and procedures that are to be followed to ensure security, confidentiality, integrity, responsible use and availability of the SASSETA data and information from unauthorised access. All the SASSETA users, partners and stakeholders are also responsible for protecting all the information technology resources, data and information.

7 Policy Objectives

The objectives of this policy are as follows:

- To support the organisation's strategy relating to cyber and information security;
- To establish the responsibility and accountability in SASSETA pertaining to information security;
- Preservation of SASSETAs data and information resources to ensure availability, integrity and confidentiality; and
- To define processes to ensure that only authorised users have access to information systems and resources.

8 Applicable and related policies and inclusions

8.1 Related policies

The following policies and procedures are related to the Information Security Policy:

- Acceptable Use Policy
- Backup and Restore Policy
- Change Management Policy
- User Account Management Policy
- Patch Management Policy
- Vulnerability Management Policy

8.2 Applicable policies and inclusions

Where no other policy has been developed or approved, this policy will also cover and include the following policies

- Antivirus configuration and management policy
- Firewall configuration and management policy
- Network Infrastructure configuration and management policy
- Server Configuration and Management Policy
- Electronic Fund Transfer (EFT) Policy

9 Policy provisions, guideline and business rules - Organisational Security

9.1 General

These provisions, guidelines and business rules are applicable to systems hosted by service providers and those maintained by SASSETA. The strategic ICT service providers will be governed by the SASSETA ICT Security and related policies.

9.2 Policy Stipulations

9.2.1 Information Technology Asset management

- All ICT Assets constitute valuable government resources. Asset management defines the acceptable use and protection of information and infrastructure related assets.
- All ICT Equipment must be recorded and or tagged with an asset tag.

- A formal inventory of the ICT assets must be compiled to identify all assets and their respective values. The inventory list must be maintained and updated to ensure that all assets are recorded properly. The inventory list must include the following minimum information
    - Asset Number (Barcode or number allocated)
    - Description of the Asset
    - Name of the Owner
    - Location of the Asset
    - Business Criticality
    - Security Classification
- All employees provided with ICT equipment must take necessary care to protect the asset from damage, theft and loss. Where there is damage or loss, employees must report the loss or damage to the ICT Department within 24 hours of such loss or the reasonable earliest convenient time.
- The report must be in written format in a template provided by the organisation and describe the circumstances for the damage or loss. Failure to report the loss or damage within the stipulated time above will result in the employee being held personally liable for the damage or loss. Where there is loss, the employee must also provide the ICT department with a police case number.

9.2.2 Classification and control of information

- Information and information systems constitute valuable assets for its users and the organisation as a whole. In most cases, this information cannot be quantified yet it remains an important asset for the organisation.
- All information, including personal information created, processed, stored, transmitted, disposed (deleted or destroyed) must meet the requirements of the Protection of Personal Information Act (POPIA) .
- This information must therefore be protected by those owners and custodians during the lifecycle of the information.
- Information must therefore be accorded various levels of protection based on the sensitivity and confidentiality of the information. It is therefore the responsibility of each information owner in the information lifecycle to protect, classify, control, handle and give access to information appropriately.
- All information within the organisation must be protected against misuse, destruction, theft, leaks and any malicious intent by the owner, user and recipient.
- Any person who handles the information recklessly including, but not limited to leaking, unauthorised access, intentional and negligent [illegible] destruction to information will be held accountable and must be subjected to the disciplinary process.

- All business and related information created and managed during the information life cycle must be stored on the SASSETA servers to ensure backup and protection of that information.

9.2.3 Personnel Security

- Personnel security is the responsibility of the Human Resource Department and Auxiliary Services ; however, the following guidelines need to be considered to ensure consistency with the ICT Security policy.
- Personnel security has the objective to ensure that all employees and external resources are suitably security vetted and contracted in accordance with the information and technology security requirement of the institution and that they understand and execute their security related responsibilities.
- In order to limit security risks, cognisance should be taken of the relevant prescripts such as laws, regulations and policies, business requirements, classification of information to be accessed and perceived risks, including that of technology, throughout the entire employment/contracting cycle, from recruitment, appointment up to termination of employment/contract.
- The contractual agreement of employment must clearly state their security related role and responsibilities. During employment management should oversee that all security related prescripts and requirements are adhered to.
- In absence of a suitable security clearance e.g. whilst the official process is not yet concluded, the employee/contractor must enter into a declaration of secrecy or non-disclosure agreement.
- Management and personnel have different security responsibilities and liabilities that apply prior, during, and at the time of termination of employment. Prior to employment, the expected roles and responsibilities (including for information security) are defined and agreed. Part of the contractual agreement with the new employee includes acknowledgement of their role and responsibilities towards information security. During employment, management is responsible for ensuring that employees understand and apply information security in accordance with this policy. All employees must receive appropriate information security awareness training and education, as well as regular updates on SASSETA's policies and procedures, as relevant to their job functions.
- Upon termination of employment or during disciplinary procedures against the employee, the ICT department may restrict or remove access to information systems and ICT resources in consultation with the Human Resource department.

9.2.4 Third parties and Contractors

The security related to third parties and contractors is the responsibility of the line department allowing access to provide services on their behalf, however the following guidelines should be considered:

- Many government institutions grant access to numerous third parties such as vendors, service providers and other external parties without requiring any standardisation in terms of tools or solutions. Information security requirements for mitigating risks

associated with the third party's access to the SASSETA's assets must be in line with this policy and should be included in the SLA agreement with the third party.

- The third party are all external parties that may access, process, store, communicate, or provide ICT infrastructure components and systems for the institution's information.
- Third parties and contractors must be suitably vetted, or screened before providing services to SASSETA that requires them to access the information and information systems within SASSETA.
- The third parties or contractors are required to sign an Oath of Secrecy or non-disclosure agreement in accordance to the security requirements of the institution.
- All third parties offering services and requiring access to information systems within SASSETA must always be accompanied by an employee within the ICT department or relevant official within the other line department(s).
- No third party or contractor must be provided with any logical access to any critical information or systems of SASSETA without the authorised approval by the Accounting officer or his/her delegate.

9.2.5 Physical Security and Environmental controls (Server room)

- The objective of physical and environmental security is to prevent unauthorised physical access, damage and interference with SASSETA's information and information processing facilities.
- All information processing systems and infrastructure which includes but not limited to servers, backup devices, firewalls shall be kept in a controlled environment and secured room known as the server room.
- The server room shall only be accessed by authorised personnel and the ICT Manager or Head of Department shall grant such access.
- The server room shall have a minimum of the following infrastructure installed, raised flooring, air-conditioning, fire suppression system, Uninterrupted Power Supply (UPS) and approved cabinets. All infrastructure shall be serviced on a regular basis (at least bi-annually) and a record of service for each infrastructure component shall be kept in the server room.
- The access door to the server room shall be fitted with an access control system that can record all persons entering the server room. A visitor sign in register shall be kept to record all persons entering the server room including authorised persons from the ICT department.
- The server room should be fitted with fire and water detection equipment to monitor and manage the environment against disaster related to fire and water.
- All equipment in the server room shall be recorded in line with the provisions of paragraph 9.2.1 above.

9.2.6 Acceptable Use

- The purpose of this policy is to firstly establish guidelines and minimum requirements governing the acceptable use of Information Technology Resources application systems

utilised by SASSETA and the acceptable use and safeguarding of the Information Technology assets. Refer to the Acceptable Use Policy for detailed requirements.

9.2.7 Password Management

This section must be read and implemented in conjunction with the User Account Management Policy, where provision has been made in the User Account Management Policy and have not been made here, they will also be applicable and vice versa or mutatis mutandis:

- Passwords must be utilised on all systems within SASSETA to protect the confidentiality and integrity of such systems. All systems within SASSETA must be accessed using passwords. This include Integrated Management Information System (Indicium), Enterprise Project Management System (EPM), GreatPlains Dynamics, SmartHR (HR system) Email, Active directory (Shared Folders), DataProof (Document Management System), Issabel (Call Centre System) and any system to be developed or installed in the future.
- All SASSETA users must keep all passwords confidential and must under no circumstances share or divulge user names and passwords. Where possible new users must be provided with a secure temporary password, whereafter the password is amended to comply with SASSETA passwords standards.
- Passwords must not be documented and stored in an unsecure environment.
- No users or employee must attempt to find out another user's password or gain access to systems using another user's account/credentials.
- No passwords must be saved in an electronic document unless it is encrypted.
- No passwords must be sent using emails.
- Passwords and usernames must not be written on keyboards, walls, monitors, post-it notes, table or easily accessible material.
- Users are only allowed to use one username for each system that they access.
- Users are required to log out of all systems, including network when not in use including after hours.
- When a user is not making use of their computer, the user must lock the computer by using the password protected screen saver, locking the desktop or logging out of the computer.
- Users are required to report any misuse or unlawful use of User ID's and passwords to the Helpdesk, who will record it as a security incident and escalate it to the ICT Department through the incident management process.
- User passwords must be changed immediately if compromise is suspected.
- Unsuccessful logging attempts should be logged and investigations should occur where unsuccessful logging attempts are out of the normal range.
- Sensitive System Administrator passwords should be sealed and kept in a secure location.

9.2.8 Server Security and Configuration Management

- SASSETA should maintain a Server registry database that must be registered within the ICT business unit. At a minimum, the following information needs to be maintained:

- Server location;
- Hardware and Operation System/Version;
- Main functions and application, if applicable;
- The system administrators; and
- The system owners.
- Business Criticality

- The Servers must be kept up-to-date by developing the most critical and recent system and security updates, and installing the latest service packs. (An Automated Patch Management solution must be installed to automate the process.)
- Configuration changes for servers must follow the appropriate change management procedures.
- The servers must be installed, scanned and updated with the latest antivirus software.
- The applications hosted on the servers must be kept up-to-date.
- The servers hosted by SASSETA must be physically located in an access-controlled environment.
- Installation must be done on a clean system; upgrading a system will keep leftover registry entries and other remaining data that could affect stability and security.
- Only one operating system on the server must be installed. This is to ensure that an attacker/hacker cannot bypass security settings on the operating system.

Access to Operating Systems

- All information resource users, including system administrators, must be uniquely identified on each system accessed. System access must be restricted to a need-to-know basis, and requires prior authorisation from the Information Owner.
- The access requirements are defined in the User Account Management (UAM) Policy and Procedures of SASSETA and should be adhered to in all circumstances.
- Access to operating systems must be restricted to authorised users only, and secure logon should be used to control access.

9.2.9 Firewall Security and Firewall Configurations

- This section is designed to protect the confidentiality, integrity and availability of the SASSETA data, and to establish the standards by which SASSETA firewalls must be configured and administered.
- SASSETA's firewall platforms are required to be located in the physical server room, and that the access to the set is limited only to approved users and ICT Manager.
- All firewall devices installed and implemented must conform to the standards as determined by the SASSETA ICT department.
- All firewalls must be updated regularly with the patches and security updates as they are released.
- The firewall must be configured to deny all internet bound traffic unless explicitly permitted.
- The firewall must be configured to restart automatically and not require user interaction to commence.

- The firewall must be configured to notify the ICT Business unit in real time relating to security breaches to ensure proactive imperative action.
- The firewall must be configured to ensure that all incoming files and attachments are scanned by the antivirus.
- The firewall rules and configurations are required to be reviewed on a quarterly basis to ensure they provide the necessary levels of protection and are configured accordingly.
- Firewalls must be installed within the business environments where confidential information is captured, processed or stored.
- The firewall rule set and configurations must be backed up at regular intervals and be available for restore purposes. However, they must not be stored on the current device.
- The firewalls logs must be retained and reviewed on regular basis.
- In the event where a user requests exception to the firewall policy configuration, a formal request must be made to the ICT manager to evaluate the risk of opening the firewall to accommodate the request.
- Changes to the firewall must follow the change management policy and a change management form must be completed.
- Firewall rules must be clearly labeled and defined on the firewall for ease of reference.

9.2.10 Antivirus Control and Configuration

- All SASSETA computers and devices which connect to the SASSETA networks must ensure that the Antivirus software is installed and is configured to update and scan at regular intervals.
- All computers and ICT devices in the SASSETA environment must have the latest antivirus and definitions installed. The antivirus installed must be configured to perform updates at regular intervals.
- Only licenced antivirus software is to be installed on the SASSETA computers and laptops.
- Only authorised ICT staff is allowed to configure the antivirus software and to deploy the antivirus to SASSETA servers and SASSETA computers, laptops and other devices.
- ICT staff must ensure that antivirus is installed on all users' computers and laptops, libraries and should be updated prior to connecting to the SASSETA network.
- Users of laptops and mobile devices, computers must ensure that they log onto the active directory every time they are in the offices to allow for the updating of the antivirus software.
- The antivirus server must be configured to deploy updates to the SASSETA computers and run scans at regular intervals.
- The antivirus server must be deployed centrally and configured to manage all user policies relating to the local SASSETA virus scan settings and prevent users to alter settings, including the level of protection.
- The antivirus server must be configured to identify any SASSETA computer or laptop which was not successfully updated during an antivirus update deployment.
- If a user suspects that the computer/laptop or device has a virus, the user is required to contact the ICT business unit to notify them of the incident.
- SASSETA reserves the right to disconnect any computer, laptop or device from the SASSETA network, if deemed to be infected or suspected to host a virus.
- Virus infected computers must be removed from the SASSETA network until verification has been done to establish if virus-free by the ICT business unit staff.

- The antivirus must be configured to be quarantined prior to the deletion of the affected attachments when identifying antivirus or related malware and notify the sender and/or the recipient.
- No employee may knowingly distribute viruses or bypass any detection systems in place.
- Users are not allowed to open any e-mail or attachment if the source of the e-mail is unknown to the user.
- Individuals receiving data media (e.g. USB), from any source within or outside SASSETA have the responsibility for ensuring that it is checked for viruses before use. Similarly, individuals intending to pass on data media within the SASSETA or to external third parties must ensure that it is first checked for viruses.

9.2.11 Mobile and other technology devices

- All mobile computing devices and related technology devices must be used to ensure that the SASSETA information and data is not compromised by compliance to the Information Security policy and Acceptable Use Policy.
- Laptops and Notebooks must be secured by using an approved laptop/notebook lock.
- All users must note that it is considered as unauthorised access to the SASSETA resources when family, friends or third parties utilise SASSETA computers and related devices.
- Removable computer media, which connects to the SASSETA network or owned by SASSETA, such as Personal Digital Assistance (PDAs), mobile phones, Universal System Bus (USB) devices, etc., must comply with the security requirements detailed in this policy.
- Users must ensure that they keep removable computer media secure. Any loss or theft of removable computer media must be treated as a security breach and reported immediately to the relevant authorities.
- Only applications that either meet with the corporate security architecture or are delivered as standard on the removable devices are authorised to be used.
- Information on removable computer media must be backed up on a regular basis.
- When removable computer media is connected to any SASSETA network it must not have any additional communication sessions running.

9.2.12 E-mail, Internet and Intranet

- The users are encouraged to use E-mail, Internet and Intranet access to enhance the operations of SASSETA and to allow the users to perform their work more efficiently. Internet, Intranet and E-mail access and attendant resources are to be used solely for work related purposes.
- All E-mail, internet and intranet usage should be in accordance to the Acceptable Use Policy.

10 Reporting of security incidents

An information security incident is defined as any unauthorised action taken on government information assets that reduces, compromises, or threatens the confidentiality, integrity, availability, or non –repudiation of the data or systems themselves in terms of the ITIL Library. This includes, but is not limited to, the following:

a) Removing or bypassing existing protection and control mechanisms;

b) Using or misusing control mechanism to gain or grant unauthorised access or system privileges; or to escalate current privileges;

c) Reading, copying, modifying or deleting data by an individual or program not authorised for such action;

d) Abusing privileged access in order to monitor or impersonate another user; or reading that individuals private data without authorisation;

e) Accidental or deliberate unauthorised change of data;

f) Attempting to explore or test for security vulnerabilities in information assets when not authorised to do so; and

g) Any violation of this policy.

- All information Security related incidents should be reported to an employee's line manager and to the ICT help desk. The help desk should inform the ICT Manager and/or the person who is assigned the responsibilities of an information security officer for investigation and to take corrective action.
- Users are not under any circumstances permitted to attempt to prove a suspected weakness since this may be interpreted as a potential misuse of the system. Users are to report any observed or suspected security weaknesses in or threats to SASSETA systems or services.
- All system owners must report all significant security related physical and environmental changes to the ICT Manager promptly. Such changes include changes of physical access, changes of security responsibilities and changes of established security measures.

11 Monitoring of the SASSETA systems and users

- System administrators should ensure that where systems and applications have the capability to log events, the following should be enabled as a minimum requirement:
    - The account logon;
    - The user ID;
    - The date and time of the event; and
    - The actions taken by administration or special privileged users.
- Audit trails, user functions, and system administrator activities should be reviewed in accordance with the User Account Management Policy.

- Access violation logs (AD, LAN, WAN, Security and SASSETA applications) should be reviewed at regular intervals to identify unauthorised access or attempts.

12 Change Management and Maintenance

- The SASSETA change management policy is to ensure that standardised methods and procedures are used to alter the environment to minimise the risk for negative impact of change.
- A formal change needs to be submitted to the ICT Manager to ensure all changes in the Information Technology environment of the SASSETA are reviewed, prioritised and approved.
- All changes (infrastructure, application systems, operating systems and network related) will be managed in a controlled manner.
- SASSETA data and systems managed by the SASSETA strategic ICT service providers will be governed by the Change Management Policy of SASSETA and this clause should be included in the SLA with the service provider.
- All changes would adhere to the SASSETA Change Management Policy, including emergency changes.

13 Business Continuity Management & Disaster Recovery

- SASSETA must establish a Business Continuity Plan (BCP) to confirm that all critical business activities are available and to continue normal operations when unexpected events arise.
- The BCP must contain all information security requirements relating to SASSETA, and contain all agreed business objectives and priorities. The Disaster Recovery Plan (DRP), which is a component of a BCP must be formulated and tested. Once a disaster occurs, the DRP would initiate the restoration of ICT critical business processes to assist the organisation in returning to normal business operations.
- The BCP and DRP must be aligned and updated with changes which are experienced within the SASSETA business and ICT operations.

13.1.1 Backup and Restore

- The specific purpose of the Backup and Restore Policy is to establish controls to ensure that regular backups are maintained and are recoverable in the event of equipment failure, intentional destruction of data, or disaster.
- Backups of SASSETA should be in accordance with the backup strategy defined in the SASSETA Backup and Restore Policy.

14 Disposal of Information Technology assets

- The computers, storage components and removable storage media that contain or have ever contained SASSETAs information must be disposed of in a secure manner. The ICT business unit must ensure that all items identified for disposal must have all data removed and the necessary actions taken to ensure that no data is recoverable by third parties.
- All disposals of assets must be in accordance with the SASSET Asset disposal requirements.

14.1.1 Software

- SASSETA utilises approved legal software in support of its business operations, and respect and adhere to all computer software copyrights.
- Unauthorised and unlicensed software is prohibited from SASSETA systems and network.
- Software assets will be reviewed quarterly to establish legality and compliance requirements.

14.1.2 Software Configuration Policy

- The SASSETA software may only be configured by the ICT support staff and approved application support service providers, in support of the SASSETA business operations.

14.1.3 Telephones/Smartphones

- SASSETA will provide authorised employees communication and data devices for business related purposes to enhance the operations and productivity.

15 Roles and Responsibilities, Accountability and Sources of Authority

The roles and responsibilities are as follows:

15.1 The SASSETA Information Security Forum/ICT Steering Committee

- The responsibility relating to information security is shared throughout SASSETA. The SASSETA management should establish a forum to promote and support the security initiatives by providing adequate resourcing. The responsibilities of the forum and its members should be defined.

15.2 The allocation of the responsibilities of an Information Security Officer

SASSETA should formally appoint an Information Security Officer or delegate the responsibilities to manager(s) or service providers. The Information Security Officer responsibilities and authority should be clearly defined to ensure the alignment of the security activities with the organisational objectives.

The following are the responsibilities of the Information Security officer

- Advising the organisation on information security technologies and related issues;
- Reviewing and updating the policies and procedures relating to the information technology environment;
- Investigating the security related incidents;
- Establishing information security awareness within the organisation;
- Conducting regular information security risk assessments, and updating the ICT risk register with the risks identified in relation to information security;
- Ensuring that remote users are required to be authenticated in order to utilise external connections; and
- Monitoring compliance concerning information security.

15.3 The ICT Business Unit

I. The ICT business unit's primary focus is to support and maintain the Information, Communications and Technology infrastructure, devices and software, taking into consideration the information security of SASSETA.

II. To provide helpdesk support to computer users and assist the organisation in information security related issues.

III. To maintain a formal Service Level Agreement (SLA) with service providers for any ICT or information security related outsourced services. Ensuring that reporting or minutes of meetings are maintained to report on services rendered, as defined in the SLA.

a) SASSETA Managers

I. The managers should familiarise themselves with the Information Security Policy and supporting policies to ensure that all applications which are their responsibility have:

- A formal system administrator assigned; and
- The necessary controls are in place to ensure authorised access.

b) ICT Manager/Specialist

I. The ICT Manager/Specialist is responsible for:

[redacted] issues;

- Reviewing and updating the policies and procedures relating to the information technology environment;
- Investigating the security related incidents;
- Establishing information security awareness within the organisation;
- Conducting regular information security risk assessments, and updating the ICT risk register with the risks identified in relation to information security;
- Ensuring that remote users are required to be authenticated in order to utilise external connections; and
- Monitoring compliance concerning information security.

c) **SASSETA "Users"**

I. The responsibility of users relating to information security is as follows:

- Users should refrain from infringing software copyrights;
- Users should not attempt to access privileged accounts or data;
- Users should not share user accounts or passwords;
- Users are responsible for their own user accounts and passwords.
- All communications should be conducted in a professional way and should for no reasons interfere with his/her productivity; and
- Users are responsible for the content of information (images, text and used audio) communicated through e-mail and the internet.

16 Policy Implementation

The ICT Business Unit and Corporate Services is accountable and shall also be responsible for its future amendments or reviews.

The CEO is accountable for the overall policy implementation and reserves the right to intervene and take necessary steps when the policy is not adhered to. The accountability may be delegated to the Corporate Services Executive Manager or any other manager deemed fit for the function. Business Unit Heads, in consultation with ICT, are responsible for policy implementation in their respective divisions.

17 Non-Compliance to the Policy

The policy should be used in conjunction with the SASSETA Disciplinary Policy, where disciplinary action could be a consequence due to non-compliance.

18 Policy Validity

This policy will be effective from the date of approval. In an event of any doubt about the authenticity of a policy document, the document signed by the CEO shall be considered as the only document with validity, authority and a force of law.