Acceptable Use Policy

Version 1.4 July 2021

Version Control and Approval			
Document Name	Acceptable Use Policy		
Document Number/Version	1.4		
Status/Revision History			
Rev #	**Revision Update**	**Revised By**	**Date**
1.1	New	Author: William Nkuna	January 2017
1.2	Revision	William Nkuna	June 2018
1.3	Revision	William Nkuna	November 2019
1.4	Revision	Mpumelelo Khumalo	July 2021

Approval	
Date Approved	
Date Last Amended	July 2021
Date of Next Review	2023/24
Related Policies	Information Security Policy, User Account Management Policy

Authored By	
Name	Mr. Mpumelelo Khumalo
Position	Acting ICT Manager
Signature	Date: 30/08/2022

Reviewed and recommended by	
Name	Ms. Sibongile Ngwenya
Position	Executive Manager: Corporate Services
Signature	Date: 30/03/2022
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) Acceptable Use Policy is developed to protect employees, management and SASSETA stakeholders utilising its systems and ICT infrastructure from unlawful, damaging or destructive actions, which may be performed intentionally or unintentionally. It is not aimed at restricting anyone from the culture of openness, trust and integrity.

The computer equipment, network infrastructure and all application systems utilised by the employees, temporary staff, portal users, interns and contractors are to be used in the normal business operations, in serving the interests of the company, and of our stakeholders.

The following stakeholders were consulted in the development of the policy:

- SASSETAs current ICT Business Process Owner;
- SASSETAs ICT staff
- SASSETAs Strategic ICT Service providers
- SASSETAs Management
- SASSETAs ICT Steering Committee
- SASSETAs Audit and Risk Committee

1.1 Purpose

The Purpose of this Policy is to regulate and manage the users of SASSETA information systems on the acceptable use of information technology hardware, software, network, infrastructure and related systems.

1.2 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by the employee or a third party.

This policy applies to all employees of SASSETA, contractors, vendor support staff, interns and temporary staff or external stakeholders who utilise computer equipment, network infrastructure and all application systems.

1.3 Definitions and Terms

Term/Acronym	Definition
User ID	A unique identification code to distinguish one user from another.
Information Technology Resources	The computer equipment, software, network, infrastructure, data .and information.
ICT Manager	The person responsible for managing, directing the ICT operations.
Online Games	The social phrase for playing computer games on the internet.

User	Any person defined as an employee, contractor, vendor support staff, stakeholder or temporary staff who has permission granted by the SASSETA management to access the ICT environment and resources.

2 Policy Statement

The Acceptable Use Policy's purpose is to establish guidelines and minimum requirements governing the acceptable use of computer equipment, network infrastructure and all operating and application systems utilised by SASSETA, whether on the premises, offsite or hosted outside the premises of SASSETA, owned or leased, and the acceptable use and safeguarding of the ICT assets.

3 Policy Objectives

The objectives of this policy are as follows:

- To provide the guidance for the acceptable use of the SASSETA ICT assets and resources;
- To ensure compliance with the South African regulations and other relevant legislation;
- To provide guidance and comply with standards and best practices;
- To ensure users have proper awareness and concern for the security of ICT resources and adequate understanding and appreciation of their responsibilities during its use;
- To ensure users are aware of their accountability and possible liability in failure to comply with the policy.
- To encourage the cost effective and productive use of the SASSETA ICT infrastructure, hardware and software; and
- To guide employees, temporary employees, stakeholders, interns and contractors in the appropriate and acceptable use of ICT hardware and software in accordance with their responsibilities associated with computer resource use.

4 Policy

4.1 Background

The Safety and Security Sector Education and Training Authority (SASSETA) Acceptable Use Policy is developed to protect employees, stakeholders and management and SASSETA as an organisation from unlawful or destructive actions, which may be performed intentionally or unintentionally.

The computer equipment, network infrastructure and all operating and application systems utilised by the employees, temporary staff, portal users, interns, stakeholders and contractors are to be used in the normal business operations, in serving the interests of the organisation and of our clients.

4.2 Legislation, Framework and related policies

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

4.2.1 Legislation

- 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 Communications and Provision of Related Information Act, 2002 (Act 70 of 2002)

4.2.2 Government Policy framework

- Public Service Corporate Governance of Information, Communication and Technology Policy framework.

4.3 Policy provisions, guidelines and business rules

The SASSETA business critical systems hosted and maintained by the SASSETA strategic ICT service providers will be aligned to the organisation's Acceptable Use Policies. The ICT service provider's policies should be audited to ensure best practice and alignment to the SASSETA business rules as per SLA. Furthermore, service provider will supply SASSETA with regular reports and evidence that will confirm that their systems comply with best practice and legislation.

4.3.1 General Acceptable Use

I. A user must not use any ICT resources in such a way that due to his/her actions cause possible harm to the ICT resources and/or reputational damage and/or liability to SASSETA.

II. A user is prohibited from compromising the security relating to the SASSETA ICT resources, including the integrity and the confidentiality of data and information.

III. A user is not permitted to use any ICT resource, for which he/she has not been formally authorised to use.

IV. A user may only use the ICT resource for SASSETA business purpose and not for any personal or commercial purpose, which is not in the interest of SASSETA business.

V. A user should refrain from unauthorised amendments of any SASSETA ICT resources configuration and security measures, including the unapproved uninstallation of SASSETA software. Furthermore, under no circumstances illegal software should be loaded on the SASSETA ICT resources.

VI. [illegible] and not share usernames and passwords.

VII. A user is prohibited from making use of any other users ID and password unless authorised by management.

VIII. Users are responsible to promptly report the theft, loss or unauthorised disclosure of any ICT resources, data and information.

4.3.2 Network

- Users are prohibited from premediating interference with the SASSETA network, which could result in unavailability of the Network or high volume of network traffic, which is not normally experienced in normal business practice.
- Users are prohibited from interfering with the SASSETA network preventing other users from conducting their tasks, except when formal approval is obtained to conduct maintenance or upgrades to the SASSETA network or network devices.
- Users are not allowed to monitor the SASSETA network traffic or contents, without formal authorisation from the ICT business Manager or CEO.
- Users are prohibited from conducting vulnerability scans on the SASSETA network.
- Users are prohibited from attempting to bypass the SASSETA network security.
- The ICT Manager has the right to prioritise network traffic to enhance business communication where necessary.
- All computers connected to the SASSETA network are subjected to:
    - Initial security scans prior to connecting to the SASSETA network;
    - Periodic security scans when connected to the SASSETA network.
- The SASSETA network may not be used for the following activities:
    - Hosting and playing of network computer games;
    - Downloading and transferring of non SASSETA movies and/or clips between SASSETA computers; and
    - Transferring of personal movies, clips and/or personal photos.
    - Downloading and transferring of pornographic material on SASSETA computers.

4.3.3 Internet

- Users are prohibited from premediating interference of the Internet.
- Users may utilise the Internet for SASSETA business purposes and should be careful of providing personal information or company information to 3rd parties.
- Users should be diligent when using data and information, to prevent wasteful expenditure and slowing down ICT resources.
- Users may not access websites which might be offensive to other employees or contain hate speech and pornographic material.
- Users should refrain from using the Internet when it hinders the employee's productivity.
- Users should not publish or post comments, upload videos or images which might be deemed as illegal or unlawful.
- The SASSETA management has the right to monitor Internet activity.

4.3.4 Email

- When receiving email attachments from unknown sources, users should consult with the ICT business unit prior to opening these documents, as they may contain viruses or related harmful source codes.
- Users are prohibited from accessing data, information or emails not intended for receipt thereof.
- Users are prohibited from attempting to intercept, amend, and delete other SASSETA users or their profiles, unless formal approval has been obtained by the ICT department.
- The SASSETA management has the right to monitor email communications.

4.3.5 Remote Access

- A user and stakeholder need to obtain formal access from his/her line Manager and the ICT Manager for remote access.
- Access to the network shall be configured to restrict the access to the specific section of the network required.
- The access to the network shall be configured to ensure that the users have specific entry points.
- The remote access shall be configured to log:
    - The duration of all the connections and sessions;
    - Logon/Log off session details.
- The ICT business unit shall ensure that external connections access should be disabled when not in use.

4.3.6 Mobile devices and other technology devices

- A user needs to obtain formal authorisation to connect any data device, or non SASSETA related devices to the SASSETA network.
- All network devices connected to the SASSETA network are subjected to:
    - Initial security scans prior to connecting to the SASSETA network; and
    - Periodic security scans when connected to the SASSETA network.
- All devices which connect to the SASSETA network need to have a password.
- Prior to copying SASSETA data on any data devices which are connected to the SASSETA network, formal approval should be obtained from the line manager.
- Copying data on any data devices which are attached to the SASSETA network, the data needs to be encrypted with a password.

4.3.7 Unacceptable Use

- All users are to refrain from utilising the SASSETA ICT resources to conduct illegal activities which is deemed unlawful in accordance with the South African legislation.
- The users of SASSETA ICT resources are to refrain from:
    - Viewing, downloading, storing and distributing pornography;
    - Utilising offensive, discriminating language that could result in civil and/or criminal actions while utilising SASSETA ICT resources;
    - Participating in threats of violence;
    - Playing computer games;
    - Downloading copyright intellectual property;
    - Downloading videos, movies, games, software or music;
    - Viewing movies, music videos, videos online;
    - Uploading of personal or SASSETA data to social sites without approval of the line manager in compliance with the SASSETA POPI Policy.
    - Introducing malicious software to SASSETA (e.g. key loggers and viruses etc); and
    - Sharing or revealing your SASSETA account password(s) to other employees or 3rd parties.

5 Roles and Responsibilities, Accountability and Sources of Authority

The roles and responsibilities are as follows:

a) The ICT Business Unit

I. The ICT business unit's primary focus is to give all authorised users access to Acceptable Use services.

II. To support and maintain the Information, Communications and Technology infrastructure and software to allow such access and use of ICT resources

III. To provide desktop support to users and assist with issues related to the use and accessing of ICT systems and infrastructure

IV. To provide necessary training relating to the acceptable use of ICT Resources and Infrastructure within SASSETA.

b) SASSETA Managers

I. The managers should familiarise themselves with this Acceptable Use Policy and supporting policies to ensure that all users within their units are familiarised with the policies.

II. Ensure that all the necessary controls are in place to ensure proper usage of the ICT infrastructure, hardware, software and systems in compliance with the policies.

III. Report all violations of this policy when it comes to their knowledge and take corrective and disciplinary measures to ensure compliance.

c) **ICT Manager**

I. The ICT Manager is responsible for:

- Advising the organisation on the implementation of this policy and related issues;
- Reviewing and updating this policy and procedures relating to Acceptable use policy
- Investigating the related breaches and incidents pertaining to the access and usage of ICT Resources and Infrastructure
- Monitoring compliance concerning usage of ICT Resources and Infrastructure.

d) **SASSETA "Users"**

I. The responsibility of users

- Users should familiarise themselves and comply with the content of this policy;
- Users should be responsible and ensure proper use of the ICT resources provided to them;

6 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 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.

7 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.

8 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.