DRAFT Information and Communication Technology Acceptable use policy

27 February 2025

Type of Document:	Policy
Purpose:	*The aim of this Policy is to provide for the safe and lawful use of Stellenbosch University's information and communication technologies.*
Approved by:	Choose an item.
Date of Approval:	Click or tap to enter a date.
Date of Implementation:	Click or tap to enter a date.
Date of Next Revision:	Click or tap to enter a date.
Related Documents:	e.g., Previous versions of the Policy
Policy Owner:	Chief Operating Officer
Policy Curator:	Chief Director: Information Technology
Keywords:	Information and Communication Technology (ICT) resources, ICT Infrastructure, Software management and usage, Information and data security
Validity:	The English version of this Policy is the authoritative version, and the Afrikaans version is the translation

TABLE OF CONTENTS

1. THE ESSENCE OF THE POLICY

This Policy addresses the need to protect the Stellenbosch University's (SU's) ICT resources and its data, while enabling students, staff, alumni, visitors and contingent workers (from here on referred to as stakeholders[1]) to do their work aligned with SU's vision.

2. INTRODUCTION

This Policy aims to guide the acceptable use of SU's information and communication technology resources (ICT resources[2]) to ensure the lawful and secure use in support of the University's activities whilst adhering to SU's values. The Policy addresses the need to protect the University's intellectual property and stakeholder(s)' data while enabling them to do their work aligned with SU's vision.

3. APPLICATION OF THE POLICY

This Policy applies to:

3.1 **All stakeholders** who connect to the university network.

3.2 **Access and usage of ICT resources** provided, arranged or facilitated (e.g. Bring Your Own Device (BYOD)) by SU to use for the University's activities.

3.3 **Processes,** that includes but is not limited to institutional, operational and academic (teaching-learning-assessment, research) processes as well as the processing of personal information.

4. PURPOSE OF THE POLICY

The policy's purpose is to define, regulate, manage, and govern the acceptable use of ICT resources at SU.

5. AIMS OF THE POLICY

To ensure that SU's use of ICT resources is aligned and compliant with IT industry frameworks, standards, and best practices and that risks are managed to protect SU's ICT resources, the policy aims to give effect to:

5.1 **Foreign and domestic law (**including the services) that are hosted or supplied by international partnerships, which are subject to the laws associated with the geographical location in which these services are hosted, e.g. Cybercrimes Act 19 of 2020, Computer Misuse Act 1990, etc.

5.2 **Third-party regulations or agreements** including the terms of engagement associated with the resources and services that SU has contracted with or has contractual software licensing agreements, e.g. EDUROAM services and the Dramatic, Artistic and Literary Right Organisation (DALRO) agreement.

5.3 **Industry-specific regulations**, e.g. the Health Insurance Portability and Accountability Act (HIPAA) and Ethics in Health Research (2015 Guidelines South Africa Department of Health).

5.4 **Institutional policies, regulations or guidelines** that provide specific rules of engagement that all stakeholders utilising ICT resources should be familiar with (available at SU Policies

[1] SU Stakeholder groups as defined in the SU annual report (e.g. in 2024 defined as students, parents and sponsors of students, staff, government, industry, donors, research foundations, investors, community)

[2] ICT Resources include the university network, servers, software and applications, cloud services or online services, hardware (printers, laptops, desktops, etc.), data, information and records, intranet, communication platforms, SU credentials (username and password) provided, arranged or facilitated by SU, access to authorized systems, etc.

and regulations).

6. POLICY PRINCIPLES

The ICT resources are provided to further SU's vision and strategic priorities. Information and data, and the technologies used to process information and data, have value. SU is committed to ensuring the safe and lawful use of its ICT resources in line with SU's values as well as leading international practices, standards and principles.

7. POLICY PROVISIONS

The policy principles listed in paragraph 6 give rise to the following binding policy provisions.

7.1 ICT Infrastructure

The ICT infrastructure is an SU asset that contributes to the ICT function and is designed to ensure the stable, sustainable, and reliable delivery of IT services.

Stakeholders should not interfere with ICT infrastructure. This includes:

7.1.1 Connecting any unauthorised device that poses a threat to ICT services, disrupts the business function of SU, reconfigures network equipment that was not approved or deliberately circumvents ICT security measures.

7.1.2 Accessing or attempting to access any system, account, or data without proper authorisation.

7.1.3 Introducing or spreading malware, viruses, or any other security threats.

7.1.4 Interfering with or disrupting the normal operation of technology resources, including intentional or unintentional actions that impact system performance or availability.

7.1.5 Accessing, storing, or distributing content that is offensive, discriminatory, or violates institutional standards.

7.1.6 Sending or responding to unsolicited emails, spam, or phishing attempts.

To ensure this, stakeholders are required to be familiar with the relevant rules and guidelines in Appendix A.

7.2 Software management and usage rights

Software management involves the acquisition, installation and maintenance of standard software applications installed on SU assets, institutional software systems, as well as software used within the faculties for academic programs. To ensure that the software usage rights are followed, software is used securely, licenses are managed in terms of the licensing models, and software versions are tracked and patched as required, stakeholders should:

7.2.1 Not engage in illegal activities such as software piracy, unauthorised distribution of copyrighted material, and fraudulent actions.

7.2.2 Keep the software and information systems up to date by applying security patches[3], operating system patches[4], software updates[5], critical updates[6], hotfixes[7] or automatic

[3] A security patch is designed to fix vulnerabilities that hackers can exploit.

[4] An operating System (OS) patch is specific to the OS (like Windows) to improve performance, fix bugs or close security gaps.

[5] A software update is a newer version of a program that fixes bugs or adds additional features.

[6] A critical update is a high-priority patch that address serious security or functionality issues.

[7] A hotfix is an urgent fix that addresses specific problems or issues.

updates[8] to protect servers, computers, information systems, operating systems, and applications from security threats. The process of patch management[9] follows a specific patch cycle to regularly schedule which patches must be reviewed, tested, and applied.

7.2.3 Use only software that the institution has licensed, either through a campus agreement, subscription, perpetual licenses, or a license model according to the software usage rights of the software/application. Installing unauthorised software is prohibited. Copying or sharing of authorised software is prohibited.

7.2.4 Not disable or uninstall antivirus software. The antivirus software installed on the devices is compulsory. The function of antivirus software is to protect against malware, viruses, and other security threats. Antivirus management therefore secures the IT ecosystem and reduces the risk of cyberattacks or data breaches by regularly updating antivirus software, performing scans, and taking action to remove threats if detected. The list of standard software installed on all SU devices is included in Appendix A.

7.2.5 Use email to support the furtherance of the SU mission and institutional purposes. See the email and communication regulation listed in Appendix A for the expectations and regulations governing email and communication services.

7.3 Information and Data Security

Information security protects the institution's ICT resources from unauthorised access, theft, damage, or loss, ensuring that sensitive information is kept safe. The principle of information security of the confidentiality-integrity-availability (CIA) is defined as follows:

- ***Confidentiality***: information/data/record(s) should only be available to those with assigned permissions authorising access to that information/data/record(s).
- ***Integrity***: information/data/record(s) is consistent, accurate, and trustworthy.
- ***Availability***: to minimise interruption, information/data/record(s) are easily accessible by authorised stakeholders even during a disruption.

During employment, studies, or various other partnerships or affiliations with SU, stakeholders may handle information/data/record(s) that come under the Data Protection Act 2018, Protection of Personal Information Act (POPI Act), General Data Protection Regulation (GDPR), or is sensitive or confidential based on a contractual agreement with a vendor, supplier or SU affiliate(s). Stakeholders must be familiar with various policies or regulations (see Addendum A for the relevant policies and regulations), specifically those relating to data breaches and the reporting of cyber incidents.

Failure to apply and explain the principles within the University's information-related policies and regulations may render the University or the individuals involved with information processing non-compliant with South African or international information-related legislation. This non-compliance may lead to fines and claims against Stellenbosch University and/or the individual(s) involved under South African legislation. Non-compliance may further expose the University to significant reputational harm, and unnecessary risk and harm to data subjects.

Furthermore, in terms of information and data security, stakeholders should:

7.3.1 Safeguard SU credentials. Stakeholders are not allowed to share their passwords, attempt to use or obtain credentials that have not been granted, or impersonate someone else when using ICT resources.

7.3.2 Be sensitive to the procession of information/data/record(s) by not:

[8] An automatic update is a patch or update installed by the system without manual action to install the latest security fixes or enhance performance.

[9] A patch is a small software update that fixes issues, improves security or adds new features to a system or application.

7.3.2.1 Infringing copyright or contravening the licensing terms for software or other material,

7.3.2.2 Attempting to access, delete, modify, or disclose information belonging to other people without their permission,

7.3.2.3 Creating, downloading, storing or transmitting unlawful material, or material that is indecent, offensive, threatening, or discriminatory.

7.3.3 Engage responsibly in social media without tarnishing the institution's reputation. Any offensive material will be removed from institutional systems. The communication regulation lays the foundation for the range of SU communication-related documents.

7.3.4 Use AI responsible and ethically.

8. POLICY CONTROL

8.1 Roles

8.1.1 The owner of this policy document is the Chief Operating Officer, whose role is to:

8.1.1.1 oversee the development of the policy,

8.1.1.2 ensure that the necessary documents are drawn up,

8.1.1.3 appoint a curator for the policy,

8.1.1.4 ensure that the curator functions effectively, and

8.1.1.5 appoint a task team for the periodic revision of the policy document, as required.

8.2 The curator of this policy document is the Chief Director: Information Technology, who is responsible for:

8.2.1.1 the formulation, approval, revision, communication, release and monitoring of the policy document,

8.2.1.2 implementation of this policy document,

8.2.1.3 the interpretation of and guidance regarding the implementation of the policy, and

8.2.1.4 convening a task team to revise the policy periodically as required.

8.3 Implementation

The Information and Communication Technology Acceptable Use Policy regulates the use of ICT resources at SU. Within this context, the IT division develops and continually updates its guidelines, rules and regulation.

8.4 Monitoring and Reporting

SU may monitor and log the use of its information and communication technologies, including personal use, for the purposes of:

8.4.1 The effective and efficient planning and operation of the information and communication technologies,

8.4.2 Detection and prevention of infringement of this policy,

8.4.3 Investigation of alleged misconduct.

The COO is accountable for creating the necessary controls to monitor and report on this policy. The curator is responsible for carrying out such measures of control.

The IT Committee monitors the implementation of the policy by means of regular reports to the

Rectorate and reports to Senate and Council as required.

8.5 Release

This policy is a public document, which is published on the SU website. The policy is approved by the Council of the University after consultation with all faculty boards, Senate, and the Institutional Forum.

Sections 11, 12 and 13 and the Addenda of this policy may be updated editorially as new definitions, policy documents and guidelines, rules and regulations arise, with approval given by the IT Committee and reported for information to the Rectorate and Senate.

8.6 Revision

This policy is reviewed every five years, or sooner if deemed necessary.

9. NON-COMPLIANCE AND INFRINGEMENT OF THE POLICY

Infringing this policy may result in sanctions under the University's disciplinary processes. Stellenbosch University may also act, as allowed by contractual agreement or relevant legislation, against members of institutional statutory bodies and third-party suppliers and vendors for non-compliance with this Policy.

Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations and third parties whose policies have being breached. In this respect, Stellenbosch University will comply with lawful requests for information from government, regulators, and law enforcement agencies. SU reserves the right to recover any costs incurred because of an infringement from the individual or entity responsible for the infringement.

Stakeholder(s) must inform the curator of the policy if they become aware of infringement(s) of this policy.

10. CONFLICT SETTLEMENT

Conflicts within this policy are to be resolved along the normal line management channels within the existing SU structures, such as the IT Committee, Rectorate and Senate itself. The final decision authority for this policy resides with the SU Council.

11. DEFINITIONS

11.1 "**SU Assets":** Assets on the SU asset register.

11.2 **"BYOD":** Bring your own device, also called bring your own technology, bring your own phone, and bring your own personal computer. This refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device.

11.3 **"Contingent workers":** Freelancers, independent contractors, consultants, or other outsourced and non-permanent workers who are hired on a per-project or ad hoc basis.

11.4 **"CUA":** Computer User Area

11.5 **"Eduroam"**: The secure, world-wide roaming access service developed for the international research and education community. It allows students, researchers, and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions.

11.6 **"ICT":** Information and Communication Technology

11.7 **"ICT resources":** Includes the university network, servers, software and applications, cloud services or online services, hardware (printers, laptops, desktops, etc.), data, information and records, intranet, communication platforms, SU credentials (username and password) provided, arranged or facilitated by SU, access to authorized systems, etc.~~Hardware, software, data, network access, third party services, online services, or Stellenbosch University credentials~~

11.8 **"ICT Partner Portal":** The central point where you can log your IT-related issues without calling the IT Service Desk. Here you will also be able to keep track of the progress of your requests online.

11.9 **"Multi-factor Authentication (MFA)":** Way of ensuring that the claimed user is in control of the credential used to login. Malicious and phishing attacks occur daily, the implementation of MFA provides an additional layer of security to limit the impact of these attacks and to ensure that only authorized users have access to our systems. Simply put, MFA is a method of authentication that requires more than one verification method.

11.10 **"Person":** A natural person or a juristic person.

11.11 **"Personal information":** Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person.
- Information relating to the education or the medical, financial, criminal or employment history of the person.
- Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.
- The biometric information of the person.
- The personal opinions, views, or preferences of the person.
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.
- The views or opinions of another individual about the person.
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

11.12 **"Protection of Personal Information Act 4 of 2013 (POPIA)":** The comprehensive data protection legislation enacted in South Africa. POPIA aims to give effect to the constitutional right to privacy, whilst balancing this against competing rights and interests, particularly the right of access to information.

11.13 **"Standard software"**: Software that is installed on a computer that is a University asset.

11.13 **"SU":** Stellenbosch University

~~11.13~~11.14 **"SU Stakeholder groups":**~~.~~ SU Stakeholder groups as defined in the SU annual report (e.g. in 2024 defined as students, parents and sponsors of students, staff, government, industry, donors, research foundations, investors, community)

11.14 **"Unauthorised software"**: Software that have not been tested and vetted by IT.

Formatted: Font: Bold

Formatted: Font: Not Bold

Formatted: Font: 11 pt, Not Bold, English (United Kingdom)

12. APPENDIX A: SUPPORTING DOCUMENTS

12.1 ICT Infrastructure

Document name	Description	Status (e.g. identified, in process or approved)
Network Standards	Ensure a reliable, secure, and stable environment for SU stakeholders by providing guidelines and protocols that ensure different devices are integrated seamlessly. The reconfiguration, network extension, or server configurations are the primary responsibility of authorised system administrators.	In process
Network Security Regulation**.**	Includes the measures taken to protect the network from unauthorised access, misuse, malfunction, modification, or reconfigurations	In process
Device security Regulation	Ensures that endpoint devices like computers, laptops, tablets, or any other network-connected devices are protected from security threats; this also includes the security measure for bring your own device (BYOD) as well as mobile device management (MDM).	In process
Identity and Access Management Regulation:	Ensures that the authorised stakeholders have access to the appropriate ICT resources within SU, managing access logs, monitoring access and actions performed for compliance and security effectiveness.	Identified
Multi-factor authentication (MFA) Regulation	Requires stakeholders to provide two or more forms of verification before accessing critical systems, data, information, records, or services.	In process
Cloud Computing Regulation	The regulation for the infrastructure as a Service(IaaS), Software as a service (SaaS) or data storage ensures the reliable, secure and sustainable use of cloud infrastructure.	Identified

12.2 Software management and usage rights

Document name	Description	Status (e.g. identified, in process or approved)
List of Standard software installed on all SU devices		In process
E-mail and communication regulation		In process

12.3 Information and Data security

Document name	Description	Status (e.g. identified, in process or approved)
Password management regulation	Ensures the use of a password phrase adheres to the password requirements as stipulated in the password regulation	Approved
Data security regulation	Ensures that our data is stored, transmitted, and disposed of securely under the institution's privacy regulation, record management policy, SUN-Records retention schedule, mandatory self-archiving for research output, and research data management regulation.	Identified
Information Security Regulation	Ensure that the University information system assets are used for the purposes which they were intended, in a manner that does not interfere with the reasonable access rights of users.	In process
Information security incident response guideline	Ensures that the management of security breaches or cyber-attacks are addressed to minimize damage by securing ICT resources and ensuring recovery. The guideline outlines the detection and analysis of the incident (identify), the protection by containing the impact and effects (protect), the response, i.e. how to detect to ensure the cause is eradicated building a suitable response (respond), as well as how to recover from the incident (recovery).	Identified
Information Classification regulation	Establishes a classification framework that enables information curators to identify and classify the information for which they are responsible.	Approved
Information Curatorship regulation	Clarifies the information- governance and management responsibilities of Responsibility Centre heads; defines the role of information curators and deputy information curators; establishes the mandate for an information curators oversight committee; establishes responsibilities for defining information curator required competencies and capabilities, and establishes responsibilities to ensure the provision of adequate training for information curators.	Approved
Mandatory self-archiving of research output regulation	Facilitates the mandatory self-archiving of institutional research output.	Approved
SUN-Records retention schedule	Defines Records Management practices for physical and electronic records for SU in pursuance of legal obligations or in the	Approved

	transaction of business, ensuring that records meet all regulatory and institutional business requirements, are retained and accessible for as long as they have business value to SU after which time they are disposed of in an appropriate manner, and can be retrieved and accessed by everyone who is entitled to use them.	
Audit Trail Logging and Monitoring regulation	Ensures that audit trails are maintained and reviewed in order to reduce risks.	In process
Risk Management regulation	Guides the management of risks at SU	In progress

13. APPENDIX B: RELATED DOCUMENTS

Document name	Description	Status (e.g. identified, in process or approved)
Asset Management as part of the Finance Policy	Determines the accounting of the deployment, maintenance, upgrading, and disposal of SU ICT assets. It is part of the Finance Policy, which includes handling obsolete or redundant assets and the purchasing and tender policy and procedure. The IT Division manages SU assets to ensure that endpoints are secure, comply with software usage guidelines, and are updated regularly with the required security updates or patches.	Approved
Position Statement: Ethical use of AI in Research, Teaching, Learning and Assessment	Provides guiding principles for staff and students regarding the integration of AI into research and teaching-learning-assessment and underlines the importance of taking responsibility and being held accountable for ethical conduct in research and teaching-learning-assessment.	Approved
Research Data Management regulation	Determines the management of research data at Stellenbosch University (SU) (“the University”) to ensure compliance with legislative frameworks, as well as protecting the University and staff and research participants involved in research through the mitigation and management of inherent risks.	Approved
Privacy Regulation	Articulates the Stellenbosch University stance and understanding of privacy-related legislation; to articulate Stellenbosch University staff and student privacy-related responsibilities.	Approved
Electronic Communication Policy	Provides a framework for the use of the electronic communication facilities of Stellenbosch University	Approved

Communication Regulation	Aims to lay the foundation for a range of SU communication-related management documents; to guide communication-related conduct by SU staff and students in the public domain, to regulate institutional communication on behalf of SU and entities linked to SU; and to establish the interdependence between this Regulation and relevant governance and management mechanisms.	Approved