Stellenbosch
UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT

# Information and Communication Technology Acceptable Use Policy

Imp

Implementation date: January 2026

forward together
sonke siya phambili
saam vorentoe

# Contents

## ICT Acceptable use policy

ICT

# Information and Communication Acceptable Use Policy

| | |
|---|---|
| **Type of document** | **Policy** |
| **Purpose** | To provide standards, frameworks and guidelines for the safe and lawful use of Stellenbosch University's information and communication technologies |
| **Approved by** | Council |
| **Date of approval** | 29 September 2025 |
| **Date of implementation** | 1 January 2026 |
| **Frequency of revision, date of next revision** | Every 5 years or as deemed necessary |
| **Previous revisions** | |
| **Policy owner**[1] | Chief Operating Officer (COO) |
| **Policy curator**[2] | 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 the Policy is the authoritative version, and the Afrikaans version is the translation. |

[1] Policy owner: The head(s) of the responsibility centre(s) where the Policy applies.

[2] Policy curator: The administrative head of the division responsible for the implementation and maintenance of the Policy.

# 1. Essence of the Policy

The Policy addresses the need to protect the information and communication technology (ICT) resources and data of Stellenbosch University (SU) while enabling students, staff, alumni, visitors and contingent workers (hereafter 'stakeholders') to perform their duties in alignment with SU's vision.

# 2. Introduction

The Policy guides the use of institutional ICT resources to ensure that it is lawful and secure, supports the University's activities and adheres to SU's values. The Policy provides for the protection of the University's intellectual property and data as well as its stakeholders while enabling them to perform their duties in alignment with SU's vision.

# 3. Definitions

3.1. **Authorised software** has been officially approved for use at SU and is installed by designated ICT representatives on a device (desktop, laptop, etc.) to fulfil stakeholders' roles/functions.

3.2. **Authorised device** is an SU asset as defined in the asset management regulation in terms of cost, useful life of more than one year and detached and movable.

3.3. **Automatic update** is a patch or update initiated by the system without manual action to install the latest security fixes or enhance performance.

3.4. **Bring-your-own-device (BYOD)** is the practice of allowing SU stakeholders to use their personally owned devices to access ICT resources for work or study purposes.

3.5. **Contingent workers** are freelancers, independent contractors, consultants or other outsourced and non-permanent workers who are engaged per project or ad hoc.

3.6. **Critical update** is a high-priority update patch that resolves serious security or functionality issues.

3.7. **Computer user area (CUA)** is a designated space at the University (NARGA, FIRGA, FHARGA, HUMARGA, etc.) with devices (laptops, desktops, etc.) for use by authorised SU stakeholders.

3.8. **Device** is any laptop, tablet, smartphone, desktop computer, server or other electronic equipment, whether owned by the University or not, that may be used for conducting University business or for processing or storing information.

3.9. **Eduroam** is the secure, worldwide 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 their campus as well as when visiting other participating institutions.

3.10. **Hotfix** is an urgent fix that addresses specific problems or issues.

3.11. **ICT resources** include the SU network, servers, software and applications, cloud services or online services, hardware (printers, laptops, desktops, etc.), data, information and records, intranet, communication platforms, credentials (username and password) provided, arranged or facilitated by SU, and access to authorised systems.

3.12. **Multi-factor authentication (MFA)** requires more than one verification method, which adds a critical second layer of security when a user signs in.

3.13. **Operating system (OS) patch** is specific to the OS (e.g. Windows) to improve performance, fix bugs or close security gaps.

3.14. **Patch** is a small software update that fixes an issue, improves security or adds new features to a system or application.

3.15. **Person** is a natural or juristic person.

3.16. **Personal information** relates to an identifiable, living natural person and – where applicable – to an identifiable, existing juristic person, including:

a) information about race, gender, sex, pregnancy, marital status, national or ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language or birth;

b) information about education or medical, financial, criminal or employment history;

c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment;

d) biometric information;

e) personal opinions, views or preferences;

f) 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;

g) another person's views or opinions about the person concerned;

h) a personal name that appears with other personal information about that person, or the mere disclosure of which would reveal information about the person.

3.17. **Protection of Personal Information Act 4 of 2013 (POPIA)** is a South African law that provides comprehensive data protection. POPIA aims to give effect to the constitutional right to privacy while balancing this against competing rights and interests, particularly the right of access to information.

3.18. **Security patches** are designed to fix vulnerabilities to mitigate cyber threats and/or unauthorised access by malicious actors.

3.19. **Software** is a set of instructions, data or programs used to operate computers and execute specific tasks. It is the opposite of hardware, which refers to the physical elements of a computer. 'Software' is a generic term for applications, scripts and programs that run on a device. They are categorised in several ways and described by different terms depending on industry and locale, of which the following is a non-exhaustive list: system software, application software, programming software, middleware, device drivers, embedded software, information system, operating system, applications, plugins, add-ons, software-as-a-service.

3.20. **Software update** is a newer version of a program in which bugs have been fixed and/or to which additional features have been added.

3.21. **Subscription service** is a licensing or access model requiring a recurring fee to access the service (cloud-based resources, digital content, etc.).

3.22. **SU credentials** are the username, password and other details that are used in combination to prove the identity of a user, device or application.

3.23. **SU stakeholders** (hereafter 'stakeholders') are students, parents and sponsors of students, staff, government, industry, donors, research foundations, investors, community.

# 4. Application of the Policy

The Policy applies to:

4.1 all stakeholders who access or connect to the SU network;

4.2 access and usage of ICT resources provided, arranged or facilitated by SU for use in connection with University activities; and

4.3 processes of an institutional, operational or academic nature, processes used for the processing of personal information, et cetera.

# 5. Aims of the Policy

The policy aims to give effect to the following in order to ensure that SU's use of ICT resources is aligned and compliant with information technology (IT) industry frameworks, standards and best practices, and that risks are managed to protect SU's ICT resources:

5.1. **Foreign and domestic law** (taking into account that services hosted or supplied by international partnerships are subject to the laws applicable to the geographical location where such services are hosted), such as the Cybercrimes Act 19 of 2020 (South Africa) and the Computer Misuse Act 1990 (United Kingdom).

5.2. **Third-party regulations or agreements**, including the terms of engagement associated with the resources and services with whom SU has concluded contracts or licensing agreements, such as Department of Defence, Eduroam and the Dramatic, Artistic and Literary Rights Organisation (DALRO).

5.3. **Industry-specific regulations** setting legal or compliance requirements that apply to a particular sector or industry to ensure that safety, privacy, ethical conduct, data integrity and operational standards are maintained, such as the Health Insurance Portability and Accountability Act 1996 (HIPAA; United States of America), the Financial Intelligence Centre Act 38 of 2001 (FICA; South Africa) and the Payment Card Industry Data Security Standard (PCI-DSS; a global standard).

5.4. **SU policies, regulations or guidelines** that set specific rules of engagement with which all stakeholders using institutional ICT resources must be familiar (available on SU's Policies and Regulations webpage).

# 6. Policy principles

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

# 7. Policy provisions

The Policy principles mentioned in paragraph 6 give rise to the binding Policy provisions set out below.

## 7.1. ICT infrastructure

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 intentionally. 'Interfere' includes the following:

7.1.1 Connecting any device (desktop, switch, etc.) that poses a threat to ICT services, disrupts the business function of SU, or reconfigures network equipment that has not been approved or that deliberately circumvents ICT security measures. For these purposes, devices are divided into three types, namely 'authorised device', 'BYOD (bring-your-own-device)' and 'personal device', which are distinguished based on ownership, usage, extent of IT support, and management and security protocols, as indicated in Table 1 below. The table shows that a personal device becomes a BYOD device when it is used to access any SU resource beyond public services, such as University email, Microsoft Teams or OneDrive, or any institutional system requiring multi-factor authentication (MFA). For those services, the device is subject to the same compliance requirements as other BYOD devices, including conditional access, security controls and any data protection policies that may apply.

**Table 1: Overview of devices linked to categories**

| **Category** | **Authorised device** | **BYOD** | **Personal device** |
|---|---|---|---|
| **Ownership** | University-owned | User-owned | User-owned |
| **Primary use** | Work-related activities | Both work and personal use | Personal use only |
| **Authorised access** | Full access to all institutional systems and resources | Access to email, selected applications and services (where licensing permits) | Access to public-facing services only (e.g. website, non-sensitive portals) |
| **Access to email** | Always permitted and configured | Permitted with security controls | If used to access SU email, it becomes a BYOD and must meet compliance requirements |
| **Access to institutional systems** | Full | Limited and conditional | Not permitted |
| **IT support available** | Full support by IT Division | Limited support (e.g. for configuring email access or approved applications) | Minimal support (e.g. basic network connectivity) |
| **Device management** | Full management (encryption, antivirus, firewall, compliance policies, remote lock/wipe) | Partial management; may require conditional access policies and registration | No management or monitoring |

| | | | |
|---|---|---|---|
| **Security policy enforcement** | Full enforcement (monitoring, logging, compliance requirements) | Partial enforcement (e.g. via MFA) | No enforcement; user is responsible for device security |
| **Monitoring and logging** | Yes | Limited (restricted to University applications or access layers) | No |
| **Remote wipe capability** | Entire device, with user consent (stolen or misplaced device) | Selective wipe, with user consent (University data only) | No |
| **Compliance requirements** | Always enforced | Enforced when accessing SU resources (email, MS Teams, etc.) | None, unless accessing email – in which case the device must adhere to BYOD compliance requirements |

7.1.2 Accessing or attempting to access any information 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, disrupting or circumventing the normal operation of ICT resources, including actions that affect the performance or availability of ICT resources.

## 7.2. Software management and usage rights

Software management involves the acquisition, installation and maintenance of authorised software applications installed on SU assets (see Appendix C), institutional software systems and software used by faculties for academic programmes. To ensure that the applicable software usage licensing conditions are complied with, software must be used securely, licences must be managed according to the licensing models, and software versions must be kept up to date as required.

Where applicable, stakeholders should adhere to the following:

7.2.1 Refrain from engaging in illegal activities such as unauthorised reproduction, adaptation, distribution or other infringing activities regarding authorised software and related intellectual property and data of the University or its stakeholders.

7.2.2 Keep software and information systems up to date, where applicable, by installing security patches, operating system patches, software updates, critical updates, hotfixes or automatic updates to protect servers, computers, information systems, operating systems and applications from security threats. Patch management includes a cycled schedule of regular actions indicating which patches must be reviewed, tested and applied.

7.2.3 Comply with the licensing conditions of the authorised software (see Appendix C) that are installed on SU assets (desktop, laptop, etc.).

7.2.3.1 Installation of unauthorised software is regulated by assigning elevated rights for software installation, with an associated self-service risk assessment.

7.2.4 Refrain from disabling or uninstalling antivirus software or security protocols relating to the operating system or application. The antivirus software installed on SU devices is compulsory, as it protects against malware, viruses and other security threats. By running regular updates, performing scans and taking action to remove any threats detected, antivirus software secures the IT ecosystem and reduces the risk of cyberattacks or data breaches.

## 7.3. Information and data security

Information security protects the institution's ICT resources from unauthorised access, theft, damage and loss, ensuring that sensitive information is kept safe. The "confidentiality-integrity-availability (CIA)" information principle entails the following:

❖ **Confidentiality** – Information/data/records must be available only to persons with assigned permissions authorising such access.

❖ **Integrity** – Information/data/records must be consistent, accurate and trustworthy.

❖ **Availability** – To minimise interruption, information/data/records must be easily accessible by authorised stakeholders, even during a disruption.

Upholding the CIA principle requires the following from stakeholders:

7.3.1 Safeguard SU credentials. Stakeholders may not share their password, attempt to use or obtain credentials or use authenticating devices that have not been granted to them, or impersonate someone else when using or accessing ICT facilities and/or resources.

7.3.2 Be sensitive when processing information/data/records by not attempting to access, delete, modify or disclose information belonging to other people without their permission.

7.3.3 Use artificial intelligence (AI) responsibly, taking the following into consideration:

7.3.3.1 **Fairness** – AI systems must treat all people fairly.

7.3.3.2 **Reliability and safety** – AI system performance must be reliable and safe.

7.3.3.3 **Privacy and security** – AI systems must be secure and respect privacy.

7.3.3.4 **Inclusivity** – AI systems must empower everyone and engage all people.

7.3.3.5 **Transparency** – AI systems must be understandable.

7.3.3.6 **Accountability** – People must be held accountable for the use of AI systems.

# 8. Roles and responsibilities

## 8.1. Owner

The owner of the Policy is the Chief Operating Officer (COO), who is responsible for:

8.1.1 overseeing the development of the Policy;

8.1.2 ensuring that the necessary supporting documents are drawn up;

8.1.3 appointing a curator for the Policy;

8.1.4 ensuring that the curator functions effectively; and

8.1.5 appointing a task team to revise the Policy document periodically, as required.

### 8.2. Curator

The curator of the Policy is the Chief Director: Information Technology, who is responsible for:

8.2.1 formulating, approving, revising, communicating, releasing and monitoring the implementation of the Policy;

8.2.2 interpreting the Policy and guiding its implementation; and

8.2.3 convening a task team to revise the Policy periodically, as required.

## 9. 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 their guidelines, rules and regulations.

## 10. Monitoring, reporting and conflict resolution

10.1. SU may monitor and log the use of ICT resources for the following purposes:

10.1.1 Safeguarding SU's digital environment and data while respecting stakeholders' privacy.

10.1.2 Effective and efficient planning and operation of ICT resources.

10.1.3 Detection and prevention of infringement of the Policy.

10.1.4 Investigation of alleged misconduct.

10.2. The COO is accountable for creating the necessary controls to monitor and report on the Policy, and the curator is responsible for giving effect to such measures of control. The IT Committee monitors the implementation of the Policy by means of regular reports to the Rectorate, as well as reports to Senate and Council, as required.

10.3. Internal conflicts must be resolved following normal line management within existing SU structures, such as the IT Committee, Rectorate, Senate and Council. Conflict with external stakeholders (e.g. members of institutional statutory bodies, third-party suppliers or vendors) must be settled in accordance with the relevant policy frameworks or contractual arrangement.

## 11. Non-compliance with the Policy

Non-compliance with the provisions of the Policy may result in disciplinary action under the University's standard disciplinary procedures. SU may also act in terms of an applicable policy framework or contractual arrangement against members of institutional statutory bodies and third-party suppliers and vendors for non-compliance with the Policy.

Information about infringement may be passed on to appropriate law enforcement agencies as well as any other organisations and/or third parties whose policy frameworks have been breached, which may lead to civil or criminal liability for the individual or entity responsible for the infringement. In this respect, SU will comply with lawful requests for information from government, regulators and law enforcement agencies. SU reserves the right to recover any costs incurred as a result of an infringement from the individual or entity responsible for the infringement.

Stakeholders must inform the curator if they become aware of Policy infringements.

# 12. Release

The Policy is a public document that is published on the SU website. Council approved the Policy after consultation with all faculty boards, Senate and the Institutional Forum.

Sections 3 ('Definitions'), 15 ('Appendix A: Supporting documents'), 16 ('Appendix B: Related documents') and 17 ('Appendix C: Authorised software') of the Policy may be updated editorially as new definitions, policy documents and guidelines as well as rules and regulations arise and are approved by the IT Committee and reported for information to the Rectorate and Senate.

# 13. Revision

The Policy is to be reviewed every five years, or sooner if deemed necessary.

# 14. Reference documents

Microsoft AI. https://www.microsoft.com/en-us/ai/principles-and-approach#ai-principles

# 15. Appendix A: Supporting documents

This is a complete list of all required documentation, but some regulations may be combined and/or incorporated into existing regulations, rules and policies. We are compiling these regulations and aim to have them completed by the end of November 2025.

## 15.1. Across ICT resources

| Document name | Description | Status (e.g. identified, in process or approved) |
|---|---|---|
| IT Governance Framework Regulation | Aligns IT governance structures with institutional goals, applying industry standard frameworks (define IT governance structure and oversight). | Identified |
| IT Compliance and Audit Regulation | Ensures adherence to internal and external audits, regulatory compliance, and governance standards. | Identified |
| Identity and Access Management (IAM) Regulation | Defines identity lifecycle management, including provisioning, authentication and deprovisioning processes (control identity and access privileges). | IAM Policy reviewed and replaced with IAM Regulation<br>To be reviewed as part of the IAM Policy:<br>Interim Access Regulation<br>Internet Access Policy<br>Super User Policy |
| Digital Identity Regulation | Defines digital identity models and trust frameworks to support secure and verifiable user identity. | Identified<br>To be reviewed:<br>Electronic Identity Validation Regulation |
| ICT Business Continuity and Disaster Recovery Regulation | Ensures that SU can prepare for, respond to and recover from disruptive events with minimal impact on operations, data integrity and service delivery. | Identified for ICT systems and services |
| ICT Backup and Disaster Recovery Regulation | Ensures that critical data, systems and services can be restored in the event of data loss, system failure, cyberattack or natural disaster, thereby safeguarding business continuity and compliance. | Identified |
| Logging and Backup Procedures | Records system and user activity across ICT resources to support security monitoring, audit and compliance, operational troubleshooting, and accountability and transparency. | Reviewed and approved:<br>Audit Trail Logging and Monitoring Regulation |

| | | |
|---|---|---|
| IT Service Management Regulation | Ensures that the planning, delivery, operation and control of IT services are carried out in a structured, efficient and accountable manner that supports institutional processes. | Identified |
| IT Change Management Regulation | Governs the lifecycle of IT changes to minimise risk and disruption during transitions. | Identified |
| IT Incident Response Plan | Provides guidelines for detecting, reporting and responding to security incidents within the institution (standardise response to security incidents). | Identified |
| IT Vulnerability Management Regulation | Ensures that SU systematically identifies, assesses, prioritises and remediates security weaknesses in its IT systems, applications and infrastructure. | Identified |
| Password Regulation | Defines standards for passwords. | Approved - to be published<br>Replaces: Password Regulation of 2008 |
| Information Security Regulation | Defines the overall strategy and responsibilities for protecting institutional information assets (protect data and system integrity). | Approved 13 October 2010<br>Reviewed and approved |
| IT Procurement Regulation | Establishes a structured, transparent and accountable process for acquiring ICT services and systems. | Incorporated as part of Purchasing and Tender Policy and Procedure<br>Add all IT-related procurement |
| IT Project Management Regulation | Establishes standards and methodologies for planning and executing IT projects effectively. | Identified |
| IT Third-Party and Vendor Risk Management Regulation | Manages risks and obligations related to outsourced services and third-party vendors (control third-party IT interactions). | Identified |
| AI and Emerging Technologies Regulation | Guides responsible deployment and monitoring of AI and other emerging digital technologies. | Identified |
| Cloud Data Governance Regulation | Ensures that data stored or processed in cloud environments is protected and governed in accordance with internal and external requirements. | Identified |

| | | |
|---|---|---|
| Multi-factor Authentication Regulation | Ensures that access to sensitive systems, data and services is protected by more than one layer of authentication, thereby reducing the risk of unauthorised access and cyberattacks significantly. | In process |

## 15.2. ICT infrastructure

| Document name | Description | Status (e.g. identified, in process or approved) |
|---|---|---|
| **ICT Infrastructure Governance Regulation** | Ensures that SU's technology infrastructure (e.g. networks, servers, data centres, cloud platforms and related systems) is planned, managed, secured and aligned with strategic business objectives in a structured, compliant and risk-aware manner. | Identified |
| **ICT Architecture Principles** | Establishes a structured framework for designing, standardising and integrating SU's information and communication technology (ICT) resources in a way that ensures interoperability, scalability, security and alignment with strategic business goals. | In review |
| **Hardware Standards** | Ensures that all physical ICT equipment used by SU – such as servers, laptops, networking devices and peripherals – meets defined requirements for compatibility, performance, security and maintainability. | To be reviewed and incorporated as part of:<br>IT End-user Equipment and Media Regulation |
| **Endpoint Security Regulation** | Ensures that all endpoint devices (e.g. laptops, desktops, mobile phones, tablets, servers) are protected from cyber threats and unauthorised access, ensuring that they do not render SU's ICT environment vulnerable. | Identified |
| **Device Configuration and Hardening Regulation** | Ensures that all IT systems and endpoints (e.g. servers, desktops, laptops, mobile devices, network equipment) are configured securely to minimise vulnerabilities and protect against cyber threats. | Identified |
| **Network Security Regulation** | Ensures that SU's network infrastructure is protected against unauthorised access, misuse, disruption and cyber threats, | Identified |

| | | |
|---|---|---|
| | thereby safeguarding the confidentiality, integrity and availability of data and systems. | |
| **Wi-Fi Access Regulation** | Ensures secure, reliable and controlled access to wireless network infrastructure. | Identified |
| **Remote Access Regulation** | Governs how users connect to SU's internal systems, networks and data from external locations. | Identified |
| **Bring-Your-Own-Device Regulation** | Governs the secure use of personal devices (e.g. laptops, smartphones, tablets) to access SU data, applications and systems, ensuring both productivity and protection of institutional information. | Identified |

## 15.3. Software management and usage rights

| **Document name** | **Description** | **Status (e.g. identified, in process or approved)** |
|---|---|---|
| System Acquisition and Development Regulation | Ensures that all new systems, applications and technology solutions are designed, developed, procured and integrated securely into SU's IT environment in a way that meets functional, security and compliance requirements. | Identified |
| Software Licensing and Usage Rights Regulation | Ensures the legal, ethical and efficient use of software by SU while protecting against legal risk, financial penalties and cybersecurity threats. | Identified |
| Software Deployment Procedure and Assessment Regulation | Ensures that all software is released into the production environment in a secure, controlled and efficient manner, minimising risk to operations and ensuring compliance with organisational standards and requirements. | Identified |
| Open-source or Open-standard Regulation | Governs the use, contribution, integration and management of open-source and open-standard software at SU, ensuring legal compliance, security, interoperability and alignment with strategic goals. | Identified |
| Security Configuration Baseline Regulation | Establishes a standard set of secure settings and controls for software | Identified |

| | | |
|---|---|---|
| | applications and systems, ensuring consistency, reducing vulnerabilities and supporting compliance with security policies and regulations. | |
| Software Asset Management (SAM) Framework | Provides structured governance, control and visibility regarding the acquisition, deployment, usage, maintenance and retirement - including lifecycle management - of software assets at SU, ensuring legal compliance, cost efficiency and reduced security risk. | Identified |

## 15.4. Information and data security

| Document name | Description | Status (e.g. identified, in process or approved) |
|---|---|---|
| Data Loss Prevention Regulation | Safeguards sensitive, confidential or regulated data from being lost, leaked, misused or accessed by unauthorised individuals, whether through accidental, negligent or malicious actions. | Identified<br>Should be aligned with:<br>Privacy Regulation<br>Record Management Policy<br>SUN-Records Retention Schedule<br>Information Classification Regulation<br>Information Curatorship Regulation |
| Master Data Management (MDM) Regulation | Ensures that critical business data is defined, governed and maintained consistently across SU, enabling data integrity, operational efficiency and informed decision-making. | Identified<br>Aligned with:<br>Record Management Policy<br>SUN-Records Retention Schedule |
| Data Governance Regulation | Establishes a formal framework for managing the availability, integrity, security and accountability of data across SU, ensuring that data is treated as a strategic asset and used in a way that supports compliance, decision-making and operational efficiency. | Identified<br>Should be aligned with:<br>Privacy Regulation<br>Records Management Policy<br>SUN-Records Retention Schedule |

| | | |
|---|---|---|
| | | Information Classification Regulation |
| Data Breach Procedure and Response Plan | Ensures a timely, structured and effective response to actual or suspected data breaches with the aim of minimising damage, restoring security and fulfilling legal and regulatory obligations. | Identified |
| Data Encryption Regulation | Ensures that sensitive, confidential or regulated information is protected from unauthorised access, disclosure or tampering – both in storage (at rest) and during transmission (in transit) – by employing approved encryption methods. | Identified |

# 16. Appendix B: Related documents

This list comprises existing policies, regulations, legislation and other documents that may assist with understanding the Policy.

| Document name | Description | Status (e.g. identified, in process or approved) |
|---|---|---|
| Asset Management as part of the Finance Policy | Determines the procedure to account for the deployment, maintenance, upgrading and disposal of SU ICT assets. This forms 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 protected with the required security updates or patches. | Approved<br>Review:<br>Finance Policy: Handling of Obsolete and Redundant Assets<br>Finance Policy: Recycling of Printer Cartridges |
| Asset Management<br>Tera Term: EBR001P - Management of moveable assets | Outlines Stellenbosch University's (SU) Asset Management lifecycle consisting of procuring an asset using the Procurement module in Oracle Cloud Financials (OCF) and managing the asset in Tera Term (TT) after asset addition, has been completed. | Approved October 2024 |
| General Code of Conduct for the Use of Lab Facilities | Previously the Code of Conduct for Computer User Areas (CUAs) | |
| 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 |
| Risk Management Policy | Guides the management of risks at SU. | Approved 30 November 2015<br>To be reviewed |
| Finance Policy: Obtaining Goods and Services | Contains general information on obtaining goods and services, the functions of the Purchasing and Provision Services Division, and keying in requisitions on SU's financial system. | Approved 4 April 2009<br>To be reviewed |
| Privacy Regulation | Articulates SU's stance and understanding relating to privacy-related legislation, and | Approved 25 May 2022 |

| | | |
|---|---|---|
| | stipulates the privacy-related responsibilities of SU staff and students. | |
| Policy on Intellectual Property: Protection and Commercialisation | Regulates and provides for the identification, protection and commercialisation of intellectual property by SU, particularly as it may arise in the course of teaching and learning and/or research and development activities conducted at SU, and in compliance with the applicable regulatory and legislative framework. | Approved December 2022 |
| Purchasing and Tender Policy and Procedure | Contains financial guidelines and procedures with regard to purchasing of goods and services and tenders. | Approved 22 November 2022 |
| Records Management Policy | Stipulates how to maintain, protect, retain and dispose of records in accordance with fiscal, legal and historical requirements. | Approved 28 November 2016<br>To be reviewed |
| SUN-Records Retention Schedule | Serves as a tool for governing SU's hard-copy (paper) and electronic records in terms of legal, financial, research and institutional requirements. | Approved 15 February 2022 |
| Research Data Management Regulation | Regulates the management of research data at SU to ensure compliance with legislative frameworks and to protect the University, its staff and those participating in research through the mitigation and management of inherent risks. | Approved 24 November 2023 |
| Communication Regulation | Lays the foundation for a range of SU communication-related management documents, guides communication-related conduct by SU staff and students in the public domain, regulates institutional communication on behalf of SU and entities linked to SU, and establishes link with other relevant governance and management mechanisms. | Approved 22 March 2023<br>To be reviewed and aligned with Email and Communication Regulation, Social Media and Digital Conduct Regulation, Collaboration Tools Regulation, Electronic Communication Policy (2003 - to be retired) and Academic Freedom Position Statement |
| Email and Communication Regulation | Defines standards for professional use of institutional email and communication tools. | |
| Social Media and Digital Conduct Regulation | Provides a framework for responsible engagement on institutional social media platforms. | |

| | | |
|---|---|---|
| Collaboration Tools Regulation | Controls the use of collaboration platforms such as Teams and Zoom to ensure data privacy and productivity. | |
| Electronic Communication Policy | Provides a framework for the use of SU's electronic communication facilities. | |
| Glossary of Terms | Defines and describes various types of governance and management documents and indicates responsibility for approval. | Approved 1 December 2003<br>To be updated |
| 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 SU 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 the competencies and capabilities required of information curators, and establishes the responsibilities for ensuring the provision of adequate training for information curators. | Approved 22 May 2022 |
| Mandatory Self-archiving of Research Outputs Regulation | Facilitates the mandatory self-archiving of institutional research output. | Approved 25 May 2022 |
| Policy on Policy Management | Establishes process for policy creation and review. | Approved 1 December 2014 |

# 17. Appendix C: Authorised software

The table below contains the authorised software approved for use on SU-owned devices to enable the fundamental software environment. The full list will be published in a software portfolio. The authorised software is primarily aligned with the Windows operating systems, although the use of Linux and Apple macOS platforms may be permitted where required by a specific job role or function.

### Operating system:

| Software name | Description |
|---|---|
| **Latest approved Windows operating system** | Software that manages a computer's hardware and software resources, serving as an intermediary between the user and the computer. |

### Software:

| Software name | Description |
|---|---|
| **Microsoft 365 Applications for Enterprise x64** | Subscription service providing the latest versions of familiar Office desktop applications such as Word, Excel, PowerPoint and Outlook, along with other applications and services. |
| **Skryfgoed** | Collection of electronic proofing tools for Microsoft® Office. |
| **Adobe Acrobat Pro** | Software for creating, editing, managing, and printing PDF files. |
| **Citrix Secure Access** | Provides secure remote access to institutional resources for users on various devices and operating systems. |
| **Tera Term** | Provides access to system used by SU for its financial and administrative operations. |
| **Teamviewer/Remote Help** | Provides access to remote support for endpoints. |
| **IBM SPSS Statistics** | Statistical analysis software used for complex data manipulation, predictive analytics, and reporting. Widely used in social sciences, education, and research. |
| **Statistica** | A data analysis and visualisation tool that offers advanced statistical procedures, predictive modelling, and machine learning capabilities. Often used in scientific and industrial research. |
| **SAS (Statistical Analysis System)** | Software tools for data management, advanced analytics, business intelligence and statistical analysis, commonly used in academic, healthcare and enterprise environments. |
| **Microsoft Edge** | Default web browser developed by Microsoft. It is available for Windows, macOS, iOS, iPadOS and Android. |
| **Google Chrome** | Fast, secure and widely used web browser that supports modern web technologies and seamless integration with Google services. |
| **Mozilla Firefox** | An open-source web browser known for its strong focus on privacy, security and user customisation. It supports a wide range of web standards and extensions. |