UNIVERSITEIT
STELLENBOSCH
UNIVERSITY

IT Enduser Equiment and Media Regulation

Type of Document:	Regulation
Purpose:	This regulation establishes rules for the appropriate use of end-user equipment and media in the Stellenbosch University environment in order to protect the confidentiality and the integrity of academic and institutional information and applications as well as the availability of services at the University.
Approved by:	SU Council
Date of Approval:	2015/06/01
Date of Implementation:	2015/06/01
Date of Next Revision:	As required
Date of Previous Revision(s):	None
Policy Owner[1]:	Senior Director: Information Technology
Policy Curator[2]:	Senior Director: Information Technology
Keywords:	End-user Equipment, Media, Academic Information, Institutional Information
Validity:	In case of differences in interpretation the English version of this policy will be regarded as the valid version.

SU Policies are available at www.sun.ac.za/policies

[1] Policy Owner: Head(s) of Responsibility Centre(s) in which the policy functions.

[2] Policy Curator: Administrative head of the division responsible for the implementation and maintenance of the policy

UNIVERSITEIT·STELLENBOSCH·UNIVERSITY
jou kennisvennoot • your knowledge partner

Information Technology (IT) end-user equipment and media regulation

Reference number	0609-EUD
Purpose	This regulation establishes rules for the appropriate use of end-user equipment and media in the Stellenbosch University environment in order to protect the confidentiality and the integrity of academic and institutional information and applications as well as the availability of services at the University.
Date of implementation	1 June 2015
Review date	1 June 2015
Previous reviews	-
Regulation owner	Senior Director: Information Technology
Regulation curator	Senior Director: Information Technology
Date of approval	
Approved by	
Exclusions	5.2.4: The IT Division is unable to provide storage space for all academic and institutional information and data at present.

1. Purpose

This regulation establishes rules for the appropriate use of end-user equipment and media in the Stellenbosch University (hereafter “University”) environment in order to protect the confidentiality and the integrity of academic and institutional information and applications as well as the availability of services at the University.

This regulation specifies the University and individual user responsibilities for processing, managing, and securing academic and institutional information on University and privately owned devices.

2. Scope

The regulation applies to all staff, students and associates who access the University network and information. The regulation relates to University owned or privately owned end-user equipment that will be used to connect to, access and/or process academic and institutional information.

3. Definitions

Refer to the *IT policy and regulation definitions* document for a description of terminology used in this regulation.

4. Related policies and documents

This regulation is one of a cluster of policies and regulations related to the protection of information technology (IT) infrastructure and information assets. It is subordinate to the *Information Security Regulation.*

5. Provisions

5.1 Access Control

5.1.1 Prior to initial use via a physical connection to the University internal network or related infrastructure, all end-user equipment (with the exception of devices that are used to connect via Virtual Private Network (VPN)) must be registered with the University's Information Technology (IT) Division.

5.1.2 The IT Organisation reserves the right to:

5.1.2.1 Refuse, by physical and non-physical means, the ability to connect privately owned or non-sanctioned end-user equipment to the University Network. The IT Organisation will engage in such action if it feels such equipment is being, or may be, used in a way that puts the University's systems, information or users at risk.

5.1.2.2 Summarily ban the use of a privately owned end-user device at any time. The IT Organisation need not provide a reason for doing so, as protection of the University Network and information is of the highest priority.

5.1.2.3 Physically disable communication ports (such as Universal Serial Bus (USB) ports, other ports that can connect to storage devices) on University-owned IT assets to limit physical and virtual access to University systems and information.

5.1.3 Users who wish to connect privately owned or non-sanctioned end-user equipment to the University Network to gain access to University applications or information and/or the Internet must implement, for their devices and related infrastructure, appropriate and up-to-date:

- personal firewall
- anti-virus software
- anti-malware software
- any other security measure deemed necessary by the IT Organisation.

5.1.4 Users must implement physical security practices to prevent the theft or loss of end-user equipment and media, especially mobile devices, and academic and institutional information, including:

5.1.4.1 If it is absolutely necessary to leave a portable device unattended, it should be secured with a cable lock or similar security device, 5.1.4.2 Ensure that portable devices are not visible when left in a vehicle. If portable devices are left unattended in a vehicle it is recommended that they are locked in the boot.

5.1.4.3 Lock portable devices away when not in use.

5.1.5 Portable end-user media and devices that are unprotected by an access control mechanism[1] may not hold confidential academic and institutional information, nor Personal Information as defined in the *Protection of Personal Information Act*.

5.2 Security

5.2.1 The use of privately owned end-user equipment and media for information storage, processing, back up, transfer, or any other processing within the University Network is subject to compliance with the University's IT network security regulations and practices.

5.2.2 End-users should apply passwords to end-user equipment as specified by the University's Password Regulation.

5.2.3 After written approval by the relevant Departmental or Divisional Head, end-users may permanently erase confidential, personal and operationally sensitive academic and institutional information from end-user equipment and media once their use is no longer required. End-users can request the assistance of the IT Division in erasing information.

5.2.4 Information storage on portable end-user media and equipment (devices) must not replace approved storage facilities. All academic and institutional information must be stored on the approved storage facilities recommended or provided by the IT Organisation, where it is secured and is routinely backed up.

5.3 Help, support and monitoring

5.3.1 The IT Organisation will support and maintain sanctioned, University-owned hardware and software, but is not under any obligation to support or maintain privately owned end-user or unsanctioned devices, although such services may be available at a fee.

5.3.2 The end-user will not install hardware and or/software that is illegal or is not relevant to the work or study context on University-owned end-user equipment without the express approval of the IT Organisation.

5.3.3 The IT Organisation may establish audit trails in all situations it feels are merited. Such trails will be able to track the attachment of an external media device to a University-owned IT asset, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end-user agrees to and accepts that his

[1] Adequate access control mechanisms include, but are not limited to: strong passwords, PIN codes, biometric (e.g. fingerprint) mechanisms. Pattern locks are not considered adequate.

or her access and/or connection to University Network may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties or that are being used in a manner that is not deemed to be appropriate. All actions initiated by the IT Division as a consequence of an audit report, optimisation of storage space, compliance with legislation, or with a legal request will be reported in the IT Incident Register.

6. Governance

6.1 Governance structure

Changes to this regulation will be initiated by the Information Security Management Committee, whose chair, the Senior Director: IT, will then consult with the necessary line structures and forums.

6.2 Ownership

The regulation is owned by the Senior Director: Information Technology.

6.3 Approval

University regulations can be approved by the responsible line manager.

6.4 Implementation

It is the IT Organisation's responsibility to implement the regulation, with the assistance of other information curators.

6.5 Review

Regulation review will be initiated by the Information Security Management Committee as and when deemed necessary.

6.6 Roles and responsibilities

The Senior Director: IT is the officer responsible for maintaining and implementing the regulation.

6.7 Breach of Regulation

For staff, disciplinary steps will be taken in accordance with the Human Resources Division's disciplinary policies. For students, disciplinary steps will be taken in accordance to the student disciplinary regulations.