UNIVERSITEIT·STELLENBOSCH·UNIVERSITY
jou kennisvennoot • your knowledge partner

Information Technology (IT) Policy Definitions

1. Introduction

The following terminology definitions are common to and used in a number of IT policies. They are consolidated here for ease-of-use, ease-of-maintenance and to avoid unnecessary duplication.

2. Definitions

2.1. For the purposes of information and IT policies **University Network** means all network connectivity infrastructure as well as a connection via the University Virtual Private Network (VPN) facility. It can be a physical connection to the internal University network and it can be a wireless connection via MatiesWIFI or Secure. It excludes the local Stellenbosch Community Network (SCN), Internet, cellular network (e.g. 3G), on-campus Konferensie wireless network or any other connection.

2.2. For the purposes of information and IT policies, **IT Organisation** is the overarching term used for the 'distributed' organisation that includes the University's central IT Division, the Faculty IT managers and their staff (including staff in Computer User Areas (CUA)), the Library and Information Services' IT section and the Business School's IT department. The term **IT Division** refers to the central IT Division solely, which is the central, governing authority for the institutional information technology function.

2.3. For the purposes of information and IT policies, **end-user equipment** is defined as any fixed or portable device that is used by the end-user to access or process University data and is connected to the University network. These devices include, but are not limited to, desktop computers, laptop computers, tablets, mobile / smart phones, Personal Digital Assistants (PDAs), and portable media storage devices such as external hard drives and Universal Serial Bus (USB) flash drives. This end-user equipment may be:

2.3.1. University property which is sanctioned by the IT Organisation (i.e. equipment procured, issued, installed, and supported)

2.3.2. Privately owned by students, staff or associates and anyone who connects to the University network

2.3.3. University property which is not sanctioned by the IT Organisation (e.g. end-user equipment purchased by a faculty for research purposes, but not installed or supported by the IT Organisation).

2.4. For the purposes of information and IT policies **end-user media** is defined as electronic storage media, portable or otherwise, that includes, but is not limited to, disk drives, removable disks, memory sticks, flash drives, digital storage cards, 'stiffy' and 'floppy' disks, optical disks, magnetic disks and magnetic tapes. This end-user media may be:

2.4.1. University property which is sanctioned by the IT Organisation (i.e. equipment procured, issued, installed, and supported)

2.4.2. Privately owned by students, staff or associates and anyone who connects to the University network

2.4.3. University property which is not sanctioned by the IT Organisation (e.g. end-user equipment purchased by a faculty for research purposes, but not installed or supported by the IT Organisation).

2.5. For the purposes of information and IT policies, **secure areas** house and secure computing, telecommunications, network and related equipment, and include data centres, cabling distribution and network/telecommunications rooms, amongst others. The following are classified as secure areas:

2.5.1. The five **core data centres** located in the University Information Technology building, Arts and Humanities building (Faculty of Arts), Bellville Park campus, Worcester campus and Faculty of Medicine and Health Sciences (Teaching building).

2.5.2. The Computer User Area Network rooms located in the University Art and Humanities building (Faculty of Arts), Accountancy building, Engineering building, Administration A building and Faculty of Health Sciences (Teaching building).

2.6. In terms of the draft *Information Management Policy*, the following information categories and sensitivity categories are defined (refer to the draft policy for the full definitions):

2.6.1. Two overarching **information categories** are defined:

a) **Academic information** is information that comprises academic content (including library, learning materials, research output, etc.).

b) **Institutional information** is information that the University as an organisation, including its staff, students and other stakeholders, owns, or is the custodian of, as well as any information that is not classified as academic information.

2.6.2. Four categories of **information sensitivity**, in descending order of sensitivity, are defined:

a) **Confidential information** is information that was provided or is used in confidence and that may only be accessed by or shared with authorised persons on a need-to-know basis.

b) **Personal information** is a specific type of Confidential Information and is defined as information that can be used to identify an individual or information about an identifiable individual and information that is defined by relevant legislation as personal information.

c) **Operationally sensitive information** (default sensitivity) is information that is used in the day-to-day operations of the University and is classified as sensitive to very sensitive depending on the extent to which its divulgence will adversely affect the University's image or operations.

d) **Public information** is published for public or general use or is already in the public domain.