UNIVERSITY OF THE FREE STATE

POLICY

Document number	IS 1000
Document name	Information Security Policy for Users of Information
Document type	Enterprise Policy
Co-ordinating UMC member	Senior Director: ICT Services
Contact	Manager: Information Security and Compliance
Status	v2
Approved by	UMC
Initial approval date	19 September 2011
Date last amended	2 October 2012
Date amendments approved	18 February 2013
Date last reviewed	2 October 2012
Date for next review	Annually
Related policies/legislation	· Policy for Acceptable Use of Computer Resources · Electronic Communications and Transactions Act, 25 of 2002

TABLE OF CONTENTS

1. Purpose

The University of the Free State (“UFS”) acknowledges an obligation to ensure information security for all information technology data, equipment and processes in its domain of ownership and control. This obligation is shared by every member of the University.

This document will explain the need for information security and indicate appropriate levels of security through standards and guidelines.

2. Scope

All information users are responsible for complying with the relevant policies and procedures.

3. Explanatory Terms

3.1. **“Must”, “will”, “shall”**
These terms denote a mandatory requirement that must be adhered to by everyone. The only allowable deviation is through a formal exception waiver.

3.2. **“Should”**
This term denotes a highly suggested, but not mandatory, recommendation.

3.3. **“May”, “can”**
These terms denote non-mandatory recommendations.

3.4. **“UFS”**
Refers to the “University of the Free State”.

3.5. **“University”**
Refers to the “University of the Free State”.

3.6. **“Users”**
Refers to any person(s) or entity/entities accessing the UFS computer network or information.

3.7. **“Information”**
Refers to any information whether in written/printed, verbal or electronic form.

4. Information Security Responsibilities and Compliance

4.1. Every user is responsible for his or her actions as it relates to the safeguarding of UFS information assets.

4.2. Failure to comply with the information security policies or other relevant policies may result in withdrawal of the right to use systems or services and/or disciplinary action.

4.3. All suspected information security incidents, weaknesses or breaches must be reported promptly to the service desk of ICT Services.

4.4. All information users are required to indicate their understanding and acceptance of this policy.

5. Procedures, Standards and Guidelines

5.1. Procedures, standards and guidelines will be published as attachments to this policy and form an integral part of the UFS Information Security Policy and therefore define it in detail.

6. Exceptions

6.1. Exceptions to any policy statement must be approved by the Senior Director: ICT Services. All exceptions to policies shall be recorded, tracked and reviewed by ICT Services.

7. Policy Statements

7.1. Information Control and Disclosure

7.1.1. All users must take care not to share sensitive information of the UFS with unauthorised personnel or external parties.

7.1.2. In the event of loss of sensitive information, the owner of the information must be notified immediately.

7.1.3. Users must notify ICT Services of any information security problem identified on the network.

7.1.4. Any staff member that requires access to a computer not under his/her direct control must receive permission from the computer owner. The computer owner can delegate control of access to his/her computer to another staff member in writing.

7.1.5. Sensitive UFS information must not be stored on any third party cloud-based storage facilities. When sensitive information is required outside of campus the official UFS SharePoint facility must be used.

7.2. Clean Desk Policy

7.2.1. Should staff members be absent from their work spaces for known extended periods, sensitive working documents must be placed in a securely locked storage space such as a drawer. If the work space is located in an office, the office door should be locked.

7.2.2. At the end of each working day, staff must tidy work areas and make sure that sensitive office documents are stored in locked drawers.

7.3. Disposal of Computer Assets and Information

7.3.1. When disposing of paper-based sensitive information, the information must be shredded or disposed of by means of other acceptable methods.

7.3.2. ICT Services must be notified of any disposal or transfer of ownership of any computer equipment, as all information on the computer will have to be securely removed following approved procedures.