Policy of the University of the Free State on Information Security for Users of Information

UNIVERSITY OF THE
FREE STATE
UNIVERSITEIT VAN DIE
VRYSTAAT
YUNIVESITHI YA
FREISTATA

UFS
UV

June 2017

INDEX

1. Background 3
2. Purpose of the policy 3
3. Guiding principles 3
4. Scope 3
5. Acknowledgement and enforcement 4
6. Standards, procedures and guidelines 4
7. Exceptions 4
8. Definitions and abbreviations 4
9. Policy 5
   - 9.1. Information control and disclosure 5
   - 9.2. Clean desk policy 5
   - 9.3. Disposal of information assets 6
   - 9.4. Removable information assets 6
   - 9.5. Passwords 6
   - 9.6. Wireless and network access connection 6
   - 9.7. Remote access 7
   - 9.8. Software installations 7
   - 9.9. Antivirus 8
   - 9.10. Messaging 8
   - 9.11. Printers 8
10. Implementation of the policy 8
11. Resource consequences of the policy 9
12. Review procedure 9
13. Policy record 10

1. Background

The University of the Free State ("UFS") owns information that is sensitive and valuable, including, but not limited to, personally identifiable information, financial data, research data, etc. Some of the information is protected by government laws or contractual obligations that prohibit its unauthorised use or disclosure. The exposure of sensitive information to unauthorised individuals could cause irreparable damage to the UFS or members of the UFS community and could also subject the UFS to fines or other government sanctions. Additionally, in the event that UFS information are tampered with or becomes unavailable, it could impair the UFS's ability to do business.

The UFS therefore acknowledges an obligation to ensure the security of all the information, information systems, equipment and processes within its domain of ownership and control. This obligation is shared by every member of the University including staff, students, contractors and visitors.

2. Purpose of the policy

The purpose of this document is to define the appropriate level of information security required to protect UFS information, information systems, equipment and processes. It is the responsibility of each information user to apply these information security measures in order to reduce the risks associated with vulnerabilities, the exposure of UFS systems and services, and legal implications.

3. Guiding principles

The University is committed to protecting the security of its information and will do so by adhering to the following principles:

3.1. Confidentiality – ensuring that information can only be accessed by those authorised to access it.
3.2. Integrity – safeguarding the accuracy, validity and completeness of information and processing methods.
3.3. Availability – ensuring that information is always available to those who are authorised to access it to prevent disruption of the University's business operations.
3.4. Regulatory compliance – ensuring that the University meets legal requirements, including those applicable to personal data and safeguarding the reputation of the University.
3.5. Digital security mandate – ICT Services has the mandate to set the minimum requirements for digital security.

4. Scope

The policy applies to:

4.1. All information users, including staff, students, contractors and visitors, as appropriate for their respective roles.
4.2. All UFS information systems, including, but not limited to, its networks and supporting infrastructure, operation systems, application systems, databases, etc., as well as systems connected to UFS computer or communication networks.

4.3. All information (data) processed by the UFS (regardless of whether it is processed electronically or in hard copy form), information sent to or from the UFS as well as information residing on systems external to the UFS network.

4.4. All external parties that provide services to the UFS in respect of information processing facilities and business activities.

4.5. All information assets, including the physical locations from which the UFS operates.

5. Acknowledgement and enforcement

5.1. Every user is responsible for his or her actions with regard to the safeguarding of UFS information assets.

5.2. The formal disciplinary process must be followed to take action against UFS staff and students who have committed an information security breach.

5.3. Failure to comply with information security or other relevant policies may result in the withdrawal of the right to use UFS systems and resources, and/or disciplinary action, depending on the severity of the breach and the individual's relationship with the UFS (i.e. staff, student, contractor or visitor).

5.4. All suspected information security incidents, vulnerabilities or breaches must be reported promptly to the ICT Services service desk.

5.5. All information users are required to acknowledge their understanding and acceptance of this policy.

6. Standards, procedures and guidelines

Standards, procedures and guidelines must be published as supporting documents for this policy to enable information users to fulfil their information security responsibilities.

7. Exceptions

The ICT Services Management Committee (ManCo) must approve any exceptions to the information security policies, and ICT Services must ensure appropriate recording, tracking and reviewing of these exceptions. Exceptions with high risk levels should be directed to the Rectorate for decision-making.

8. Definitions and abbreviations

8.1. “Must” or “will”

These terms denote a mandatory requirement that must be adhered to by everyone. The only permissible deviation is through a formal exception waiver.

8.2. “Should”

This term denotes a highly suggested, but not mandatory, recommendation.

8.3. “May”

This term denotes non-mandatory recommendations.

8.4. “UFS” or “University”

Refers to the “University of the Free State”.

8.5. “UMC”

Refers to the “University Management Committee”

8.6. “ICT Services”

Refers to the “Information and Communication Technology Services” Department of the University of the Free State.

8.7. ManCo

Refers to the ICT Services “Management Committee”.

8.8. “RMC”

Refers to the ICT Services “Risk Management Committee”.

8.9. “VPN”

Refers to a “Virtual Private Network”.

8.10. “Users” or “information users”

Refers to any person or entity accessing the UFS computer network or information.

8.11. “Information”

Refers to any information or data, whether in written/printed, verbal or electronic form.

8.12. “Data processing”

Any operation or activity performed on data, including the viewing, collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as restriction, degradation, erasure or destruction of data.

9. Policy

9.1. Information control and disclosure

9.1.1. Caution must be taken when handling sensitive information of the UFS to avoid disclosure of such information to unauthorised staff or external parties.

9.1.2. In the event of loss of sensitive information, the data governor of the information must be notified immediately.

9.1.3. Users must notify ICT Services of any information security incident or problem identified on the network.

9.1.4. UFS information must only be stored on approved storage or UFS-approved third-party cloud-based storage facilities.

9.1.5. All information processed by UFS facilities belongs to the UFS. The UFS has the right to access such information at any time through a formal approval process.

9.1.6. A formal approval process must be followed to authorise the release of information required by investigations.

9.2. Clean desk policy

9.2.1. Users must ensure that unattended equipment has appropriate protection. Where staff members are absent from their work spaces for extended periods, sensitive working documents must be placed in a securely locked storage space, such as a drawer, and computer screens must be locked. If the work space is located in an office, the office door should be locked.

9.2.2. At the end of each working day, staff must tidy their work areas and make sure that sensitive office documents are stored in a securely locked storage space.

9.3. Disposal of information assets

9.3.1. When disposing of paper-based sensitive information, the information must be shredded or disposed of in accordance with UFS-approved methods.

9.3.2. 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 in accordance with approved procedures.

9.4. Removable information assets

9.4.1. Laptops should be secured with cable locks if possible.

9.4.2. Staff who travel should not check in their laptops together with their airline luggage.

9.4.3. Information on mobile devices such as notebooks, external hard drives and memory sticks must be encrypted. Key code protected memory sticks may be used to safeguard information not encrypted by approved standards.

9.4.4. For managed mobile devices, email, calendar and contacts may be synchronised with the device. However business-related information must not be stored or backed up on the device, unless required to conduct normal business.

9.4.5. In the event that a university-managed mobile device is stolen or lost, the user must contact the ICT Services service desk to have the security incident logged to ensure access to the device is blocked and data deleted where possible.

9.4.6. Mobile devices containing UFS information must be password protected.

9.4.7. All users must return all UFS assets, including information assets in their possession upon termination of their employment, contract or agreement.

9.5. Passwords

9.5.1. Users are responsible for their own passwords. Passwords must not be written down or stored in a readable or accessible form where it can be easily exposed or discovered by unauthorised individuals.

9.5.2. Regardless of the circumstances, university passwords must never be shared with or revealed to anyone. Users must not use usernames other than their own.

9.5.3. Passwords must not be transmitted in a readable form.

9.5.4. All users must log on to the UFS self-service facility and set up their password security questions.

9.6. Wireless and network access connection

9.6.1. Only staff members authorised by ICT Services are allowed to install any wireless or network device on the University network.

9.6.2. Staff members, students, contractors, vendors and third parties must not connect any device to the UFS network unless they comply with the security considerations as determined by ICT Services.

9.6.3. Users may not enable any network service on devices connected to the UFS network unless specifically authorised by the RMC. These services include, but are not limited to, peer-to-peer sharing applications, web services, remote control and key logger services.

9.6.4. All persons, apart from staff or third parties approved by the RMC, are prohibited from using any security-testing tools, hacking tools or methods, network packet analysers, network address spoofing or packet sniffers.

9.6.5. Users must not change or spoof an IP or physical network (MAC) address.

9.6.6. Users must not use any proxy redirectors or VPN tunnels to hide source or destination addresses.

9.6.7. Users must not disable the automatic “on resume, password protect” on the screen saver. The screen saver timeout is regulated by ManCo in accordance with audit requirements.

9.6.8. Simultaneous connection to the University network and another network (e.g. 3G connection) is prohibited.

9.6.9. Users must not cause security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data where the user is not an intended recipient, or logging on to a server or account that the user is not authorised to access.

9.6.10. Unless authorised by the RMC, users must not perform any form of network monitoring that will intercept data.

9.7. Remote access

9.7.1. Users with UFS network remote access privileges must ensure that their remote access connection is given the same security consideration as onsite connections.

9.7.2. Users must ensure that they do not violate any university policies, perform illegal activities or use the access for purposes that are not in the interest of the University.

9.7.3. Remote access may be granted to users at the sole discretion of the University, based on specific terms and conditions as determined by the RMC. Such access may be revoked by the RMC at any time, without the necessity to provide any reasons.

9.7.4. Remote access to information sources may only be permitted based on authorisation by the information owners and security considerations by the RMC.

9.7.5. Remote access to the UFS computer systems from outside the University’s facilities may only be permitted by means of remote facilities provided by ICT Services.

9.7.6. All remote access sessions must be recorded where possible.

9.8. Software installations

9.8.1. Users must not install software without prior authorisation by ICT Services. Users are accountable for all non-ICT Services managed software installed on the computer under their control.

9.8.2. Users must not disable or uninstall any University-managed and -approved security software.

9.8.3. Departments responsible for managing their own software must take the necessary steps to ensure that the software is kept up to date with relevant patches and/or security updates.

9.8.4. Unless authorised by the RMC, only computers with operating systems and software that are supported by the manufacturer through the release of security patches must be allowed on the UFS network. All other software must be under patch support.

9.8.5. Users must comply with all the internal and external rules, regulations and agreements of installed software, including cloud-based and online solutions.

9.8.6. The ICT Services Department has the right to periodically scan the network for installed software and to remove software that is not legal or deemed as a security risk to the UFS.

9.9. Antivirus

9.9.1. Users must ensure that only university-approved antivirus software is installed on their computers.

9.9.2. Users must ensure that the antivirus is not disabled or uninstalled.

9.9.3. Virus incidents detected must be reported to ICT Services in order to identify whether it is a significant risk to the University.

9.9.4. ICT Services is responsible for setting the minimum requirements for all aspects of antivirus and other malware protection software and users must comply with these standards.

9.9.5. Computers of guest users must comply with approved antivirus procedures.

9.9.6. Users must not intentionally introduce any malicious programs (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) into the UFS network or systems.

9.10. Messaging

9.10.1. Email messages exiting the facilities of the UFS are, generally speaking, characterised by limited message security. As such, users should apply good judgement concerning the transmission of information to external parties.

9.10.2. Email messages routed over public networks, such as the Internet, must contain public information only unless attached documents are encrypted in accordance with approved UFS procedures.

9.10.3. Misrepresentation, obscuring, spoofing, suppression, or modification of a user’s identity on any electronic communication system is forbidden.

9.10.4. Users are responsible for regularly reviewing proxy access to their mailbox and calendar.

9.10.5. Caution must be taken by users when opening emails and email attachments that are unexpected or emails from unknown senders. If users are uncertain about emails or attachments, they should either delete the message or contact the ICT Services service desk for support.

9.10.6. Users may not intentionally send unsolicited messages or messages containing malware.

9.11. Printers

9.11.1. Confidential information must not be sent to a network printer without an authorised person to retrieve the information upon printing. Password-protected release of print jobs should be implemented.

10. Implementation of the policy

The ICT Services Management Committee (ManCo) is responsible for the administration and enforcement of this policy.

11. Resource consequences of the policy

The following resources are required to ensure the successful implementation of this policy:

11.1. Human resources – including, but not limited to, data governors and operational data stewards.
11.2. Processes and procedures – detailed guidance on how to execute the policy.
11.3. Technology – including information security software and hardware to facilitate information security processes.
11.4. Financial – budget to procure the above-mentioned resources.

12. Review procedure

12.1. The policy must be reviewed at least annually, or when significant environmental, operational or technical changes arise that may impact the confidentiality, integrity or availability of UFS information or information resources. These changes include:

- New threats or risks associated with UFS information resources.
- Information security incidents.
- Changes to information security requirements or responsibilities (e.g. new government regulations, new roles defined by the institution, new or modified security controls implemented, etc.).
- Changes to the University's organisational or technical infrastructure that impact information resources (e.g. new network, new hardware/software standard, new method of creating, receiving, maintaining or transmitting data, etc.).

12.2. ManCo is responsible for initiating the policy review process and reviewing the content of the policy.
12.3. Where changes are made to the policy, the revised policy must be submitted to the University Management Committee (UMC) for approval.
12.4. Once the revised policy has been approved, the policy record must be updated (i.e. version number, last amendment date, etc.) and the document published on the UFS intranet. Details of the changes must be communicated to the relevant stakeholders.

13. Policy record

Document name	Information Security Policy for Users of Information
Document number	IS 1000
Coordinating UMC member	Senior Director: ICT Services
Contact person	Head: Information Security, Governance & Compliance
Status	Approved
Approved by	UMC
Date first approved	11 September 2011
Date last approved	4 September 2017
Date last amended	21 June 2017
Date for next review	Annually
Person responsible for review	Head: Information Security, Governance & Compliance
Monitoring by	ManCo
Related documents	• Policy for Acceptable Use of Computer Resources • Policy of the University of the Free State on Information Security for Data Governors and Operational Data Stewards