Policy of the University of the Free State on Information Security for Data Governors and Operational Data Stewards

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

UFS
UV

June 2017

INDEX

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, 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 has been 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 governance for all UFS information, information systems, equipment and processes within its domain of ownership and control.

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 is accessible only 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 to the university's business operations.

3.4. Regulatory compliance – ensuring that the university meets its legal requirements, including those applicable to personal data under the Protection of Personal Information Act, 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 those assigned with ownership and responsibility for implementing information security, including, but not limited to, data governors and operational data stewards as appropriate to their 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, and 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. Critical information assets, including the physical locations from which the UFS operates.

5. Acknowledgement and enforcement

5.1. The formal disciplinary process must be followed when taking action against UFS staff or students who have committed an information security breach.
5.2. Failure to comply with information security or other relevant policies may result in 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).
5.3. All data governors and operational data stewards must indicate their understanding and acceptance of this policy as well as the consequences of any non-compliance, by signing the acknowledgement of the Information Security Policy.
5.4. Data governors and operational data stewards must enforce this policy in accordance with established standards and procedures.
5.5. Information on critical systems must be monitored and preserved in a manner that allows for appropriate action to be taken in the event of non-compliance.

6. Standards, procedures and guidelines

Standards, procedures, guidelines and operating manuals must be developed to enable data governors and operational data stewards 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 review 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. “HR”

Refers to the “Human Resources” department of the University of the Free State.

8.8. “ManCo”

Refers to the ICT Services “Management Committee”.

8.9. “RMC”

Refers to the ICT Services “Risk Management Committee”.

8.10. “OCC”

Refers to the ICT Services “Operational Change Control Committee”.

8.11. “Users”

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

8.12. “Information”

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

8.13. “Data domain”

A defined section of institutional data, e.g. student data.

8.14. “Data set”

A defined subsection of data, e.g. personal data of current students

8.15. “Data steward”

Stakeholders entrusted with access to institutional data. Stewardship implies the careful and responsible management of data.

8.16. “Data governor”

A role held by a senior manager accountable for the data practices and data quality of a data domain, for planning and oversight of data management programmes, and for the appointment of operational data stewards.

8.17. “Operational data stewards”

A recognised subject-matter expert assigned responsibility for the data practices and data quality of one or more data sets.

8.18. “Data guardian”

Users who are assigned with the responsibility of protecting UFS data in accordance with the access control, data sensitivity and data criticality requirements as defined by the designated operational data stewards. The data guardian role will typically fall under the control of ICT Services.

8.19. “Management”

Refers to the person responsible for managing a relevant function.

8.20. “VPN”

Refers to a “Virtual Private Network”.

8.21. "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. Identity management

9.1.1. The UFS's contractual agreements with staff, students, contractors, vendors and third parties must state their and the university's responsibilities pertaining to information security.

9.1.2. UFS staff, students, contractors, vendors and third parties must apply information security in accordance with the UFS's established policies and procedures.

9.1.3. Information security responsibilities and duties that remain valid after termination or change of employment must be defined, communicated to the staff member or contractor concerned, and enforced.

9.1.4. The HR department must perform background verification checks on successful shortlisted candidates as part of the recruitment process. Background checks must be carried out in accordance with relevant laws, regulations and ethics, and must be proportional to the business requirements, sensitivity and/or criticality of the function and classification of the information to be accessed and the perceived risks.

9.1.5. Reputable contractors, vendors and third parties must be appointed to deliver services.

9.1.6. Procedures must be in place to ensure that undue responsibility is not placed on a single individual. At least two persons must possess expertise on important information technology functions.

9.1.7. Staff in key positions must be required to take uninterrupted holidays of sufficient length in order to exercise the university's ability to cope with unavailability and detect fraudulent activity.

9.1.8. HR and Student Administration policies, procedures and contractual agreements must be followed for the onboarding, movement and offboarding of individuals (i.e. staff, students, contractors, vendors, and third parties). These policies and procedures must, at a minimum, ensure the following:

9.1.8.1. An authoritative system must be identified for each identity type (i.e. staff, students, contractors, vendors, third parties) to ensure a single source of truth for identity information.

9.1.8.2. When onboarding a new individual, the following minimum security requirements must be implemented:

- Every individual/party requiring access to UFS information systems and resources must have a valid relationship with the UFS through a signed contract, such as an employment contract, service-level agreement or non-disclosure agreement.
- Every individual that has a valid relationship with UFS must be assigned with a unique identifier, such as a staff/contractor number that is generated via an authoritative system.

9.1.8.3. When movements occur, the following minimum security requirements must be implemented:

- An individual's identity record must be modified on the authoritative system in the event of a transfer, promotion, demotion or transition.

9.1.8.4. When terminations occur, the following minimum security requirements must be implemented:

- An individual's identity record must be terminated or locked on the authoritative system after the last working day in the event of resignation, dismissal, contract termination, retirement, etc.

9.1.8.5. In the event of a staff member going on extended leave (maternity leave, sick leave, etc.), the individual would qualify for an extended absence, which must be applied for through the approved HR process. Unless otherwise authorised, all access to business applications should be temporarily suspended for the duration of the staff member's leave.

9.1.9. A process or mechanism must be implemented to ensure an effective communication link between HR, Business and ICT Services so that all parties are timeously notified of appointments, movements and termination events. Therefore, system access must be provisioned, modified or deprovisioned accordingly.

9.1.10. A process or mechanism should be implemented to enable the synchronisation of critical identity information between authoritative systems and target systems requiring this information to ensure continued data quality.

9.2. Segregation of duties

9.2.1. Segregation of duties must ensure that no single user has exclusive control over a particular information area or business process, processes complete transactions on critical systems, or have full access to data and corresponding systems.

9.2.2. Where known segregation-of-duties conflicts exist, alternative control measures must be identified to mitigate these risks.

9.2.3. Segregation of duties must be implemented to reduce opportunities for unauthorised or unintentional modification or misuse of the university's assets.

9.2.4. All the information security responsibilities of the UFS must be defined, assigned and communicated.

9.2.5. ICT Services managers must determine and define the IT roles and responsibilities of the ICT Services department and enforce segregation of duties among ICT Services team members.

9.2.6. Operational data stewards must periodically assess their respective business processes for segregation of duties-related conflicts/risks and ensure that related system access is appropriately restricted in accordance with the segregation of duties rules.

9.2.7. System development, testing and production environments must be separated to reduce the risks of unauthorised access or changes to the production environment.

9.3. Authentication management

9.3.1. All access to UFS information systems must be controlled by a secure authentication mechanism, such as passwords, security tokens, biometrics, etc.

9.3.2. All critical systems must be configured to enforce the use of strong passwords in line with the following requirements:

- Minimum password length of 8 characters.
- Minimum password history of 12 times.
- Maximum password expiry of 90 days.

- Enforcement of password complexity by using alphanumeric, numeric and special characters.
- Account lockout threshold of a maximum of 5 failed login attempts.

9.3.3. Where applicable, technology-specific password configuration parameters should be defined in terms of technical configuration standards.

9.3.4. All system-level or generic passwords must be part of the ICT Services-administered global password management database and must be stored in a secure location, preferably in a building other than the building in which ICTS is located.

9.3.5. Access to the ICT Services-administered global password database must be strictly controlled.

9.3.6. Passwords must never be stored in an unencrypted file or database.

9.3.7. Passwords should not be hardcoded into system software unless access to the source code is controlled with similar or better security measures. Exceptions must be reported and tracked.

9.3.8. ICT Services must ensure that all users are uniquely identifiable on important IT systems. Every user account must be assigned a unique username or ID in accordance with the UFS's account-naming convention standard.

9.3.9. All critical systems must be configured to enforce the changing of temporary default passwords upon first login.

9.3.10. All requests for password resets and account unlocks must be logged with the ICT Services service desk and the requests must be recorded to ensure an audit trail.

9.3.11. The ICT Services service desk must verify the requester's identity before resetting the user password or unlocking the user account.

9.3.12. Multifactor authentication should be implemented for systems with sensitive information or a high risk factor.

9.4. User access management

9.4.1. Access control procedures must be defined and documented to enable and support the following requirements:

9.4.1.1. Standard baseline access must be predefined and pre-approved at system level for all identity types requiring access to UFS information systems and resources based on the individual's relationship with and role at the UFS.

9.4.1.2. Role-based access should be implemented for all critical systems in alignment with business roles to ensure the principle of least privilege.

9.4.1.3. Operational data stewards must perform periodic reviews of user- and role-based access to all critical systems based on the following set of criteria:

- The appropriateness of the user account (i.e. does the user still need access to the data/system?).
- The appropriateness of the roles/groups/access rights/permissions assigned to the user.
- The appropriateness of the user's access or role from a segregation-of-duties perspective (i.e. segregation of duties at a user or system level).
- The appropriateness of the role and its content (i.e. access rights or permissions).

9.4.1.4. Changes to user- and role-based access, including the creation of a new user or role, amendment of an existing user's access or role, or the removal of a user's access or role, must follow the approved UFS change control procedures.

9.4.1.5. The frequency of user access and role reviews should be determined by the volume of users or role-based access changes that occur within a specified period as well as the criticality of the system.

9.4.1.6. Review feedback must be communicated to ICT system administrators for remediation on UFS systems.

9.4.1.7. A formal user access request and provisioning process must be implemented in line with the following requirements:

- All user access requests, including new access, modifications to existing access and termination of access, must be recorded and retained in a central repository.
- All user access requests must clearly specify the following details:
  - The reason for the user's access.
  - The systems or data to which the user requires access.
  - The level of access required (i.e. roles/groups/access rights/permissions).
  - Start date from which access is required.
  - End/expiry date of access (where temporary access is requested).

9.4.1.8. All user access requests must be approved by the responsible operational data steward and/or data governor as well as the system owner. The approval and administration of user access must not be carried out by the same person.

9.4.1.9. User access administration tasks, including the following, must only be carried out by authorised system administrators following a formal process:

- Creation, disablement, deletion, reactivation, locking and unlocking of user accounts.
- Assignment of roles/groups/access rights/permissions.
- Resetting of user passwords.

9.4.1.10. Users must only be provided with access to the UFS network and network services that they have been specifically authorised to use.

9.4.1.11. System administrators must ensure timely:

- Assignment of user access upon receipt of an approved access request for new appointments.
- Modification of existing user access upon receipt of an approved access request for transfers, promotions, demotions, transitions, etc.
- Termination of user access upon receipt of an access request for resignations, retirement, etc.

9.4.1.12. The approval and administration of user access rights must not be carried out by the same person. Operational data stewards are responsible for approving user access rights, whereas system administrators are responsible for administering user access rights.

9.5. Privileged access

9.5.1. Administrators and privileged user accounts must follow the same user access management procedures as defined for normal users.

9.5.2. Privileged access must be identified across all systems to provide a basis for privileged access certifications.

9.5.3. Privileged access, such as administrator or root-level system accounts, must be controlled and should therefore be restricted to selected individuals in accordance with their job roles.

9.5.4. The use of privileged utility programs that enable the overriding of system and application controls must be restricted to authorised system administrators.

9.5.5. Access to program source code must be restricted to authorised developers.

9.5.6. All privileged access must be reviewed and certified on at least a monthly basis, and any inappropriate or dormant access must be revoked immediately.

9.5.7. Passwords for privileged accounts must be reset by authorised system administrators and should not be reset by ICT Services service desk staff.

9.5.8. Privileged account passwords must be masked and stored in a secure, encrypted database.

9.5.9. Generic accounts with privileged access should be disabled or locked where possible and only used in the event of an emergency.

9.5.10. Users requiring privileged access must be assigned their own accounts with privileged permissions to perform their day-to-day operations.

9.5.11. Controls must be in place to ensure users identify themselves when shared generic accounts is required.

9.5.12. Default passwords for generic accounts created during installation of the system must be changed immediately to unique and strong passwords.

9.5.13. Each generic account must be assigned an owner, and ownership must be documented together with the associated responsibilities.

9.5.14. Generic administrator accounts must be renamed where possible to avoid obvious identification of these high-risk accounts by intruders.

9.5.15. Security audit logs must be enabled and configured for all system administrator and system operator activities to ensure the traceability of specific individuals. These logs must be made available for regular review by an independent party.

9.6. Logging and monitoring

9.6.1. The clocks of all UFS systems must be synchronised to a single reference time source.

9.6.2. Security event logs must be enabled and configured for all critical systems and should record and retain the following information at a minimum:

- The activity that was performed.
- The person that performed the activity.
- When the activity was performed.
- The status of the activity (success or failure).

9.6.3. Formatting and storage of logs must be implemented in a manner that ensures the integrity of the logs, which should include protection against tampering and unauthorised access.

9.6.4. Appropriate privacy protection measures must be implemented for logs that may contain intrusive and confidential personal data.

9.6.5. Logs must be stored (and be immediately accessible) for a period of 6 months, after which they should be stored using an appropriate backup medium for a period of at least one year or in accordance with university or legal and regulatory requirements. In this case, the affected logs must be stored in the manner prescribed and for the applicable duration in order to comply with these requirements.

9.6.6. Logs and alerts for exceeded thresholds should be configured for the following system activities:

- Create, read, update or delete confidential information, including confidential authentication information, such as passwords.
- Initiate or accept a network connection.
- User authentication and authorisation, including the following activities:
  - User login and logout.
  - Grant, modify, or revoke access rights, including:
    - adding a new user or group

    - changing user privilege levels
    - changing file permissions
    - changing database object permissions
    - changing firewall rules
    - changing user passwords
- System, network or service configuration changes, including installation of software patches and updates, or other installed software changes
- Application process start-up, shutdown, or restart
- Application process abort, failure or abnormal end, especially due to:
    - Resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space or other resources).
    - The failure of network services, such as DHCP or DNS.
    - Hardware or software faults.
- Detection of suspicious/malicious activities, such as the output of an Intrusion Detection or Prevention Systems (IDS/IPS), antivirus solution, or antispyware solution.
- Records of successful and failed system access attempts.
- Records of successful and failed data and other resource access attempts.
- Changes to system configuration.

9.6.7. Logs should include, where relevant:

- The user or system requesting the action.
- Dates, times, and details of key events, e.g. log-on and log-off.
- Device identity or location.
- Use of privileges.
- Use of system utilities and applications.
- Files accessed and the kind of access.
- Network addresses and protocols.
- Alarms raised by the access control system.
- Activation and deactivation of protection systems, such as anti-virus systems and intrusion detection systems.

9.6.8. System administrators must not have permission to erase or deactivate logs of their own activities.

9.6.9. Information security events should be logged and analysed, using tools and processes that allow for:

- Aggregation from multiple logs and data sources.
- Correlation of logs to enrich data related to security events.
- The definition of combinations of logged activity that indicate potential risk.
- The development of reporting dashboards.
- The configuration of automated alerts.

9.6.10. The logs generated for all UFS information systems must be regularly monitored and have automatic alerts configured for any UFS information security breaches, such as unauthorised access to sensitive information.

9.6.11. The following events must be monitored on all critical information systems, where appropriate:

- Changes to system configurations, particularly security controls.
- All privileged operations, such as:
    - Use of privileged accounts, e.g. supervisor, root, administrator.
    - System start-up and stop.
    - I/O device attachment/detachment.
- Unauthorised access attempts, such as:
    - Failed or rejected user actions.
    - Failed or rejected actions, involving data and other resources.

    - Access policy violations and notifications for network gateways and firewalls; alerts from proprietary intrusion detection systems.
- Privileged system access and activities.
- Technical security component fault detection.
- Outages and faults related to insufficient resources.
- Processing faults that may indicate system tampering.
- System alerts or failures, such as:
    - Console alerts or messages.
    - System log exceptions.
    - Network management alarms.
    - Alarms raised by the access control system.
    - Changes or attempted changes to system security settings and controls.
- Authorised access, including details, such as:
    - User IDs.
    - Date and time of key events.
    - Types of events.
    - Files accessed.
    - Program/utilities used.

9.6.12. Reporting of suspicious events must be performed in a timely and effective manner, through exception reporting if possible, to ensure prompt investigation thereof.

9.6.13. Adequate mechanisms for audit trails should be implemented at a database, application and network level to enable the detection of unauthorised access and misuse of sensitive data.

9.7. Security incident management

9.7.1. Measures must be in place to minimise the damage from information security-related incidents and malfunctions by taking action, resolving reported issues, monitoring and learning from such incidents.

9.7.2. To address security incidents, a formal incident response procedure must be established, setting out the action to be taken in the event of a security incident.

9.7.3. Operational data stewards and data governors must be made aware of the security incident reporting process, and that they are required to report any information security-related incidents as soon as they are identified.

9.7.4. ICT Services must ensure that all open incidents and actions against open security incidents and weaknesses are reviewed and monitored regularly.

9.7.5. A feedback process must be implemented to ensure that an individual who has reported an incident is notified of the results after the incident has been dealt with and closed.

9.8. Security awareness and training

9.8.1. All UFS staff and, where relevant, contractors and students must receive appropriate awareness education and training and regular updates on university policies and procedures, if deemed relevant for their job function.

9.8.2. Operational data stewards must ensure that all users are provided with appropriate information security training to bolster efficiency and does not compromise information security.

9.8.3. Data governors and security personnel must receive training on an ongoing basis to ensure that their management techniques, technical knowledge and skill levels remain current.

9.8.4. Security awareness should be reinforced throughout the university through regular communication.

9.9. Mobile devices and remote access

9.9.1. The UFS must adopt appropriate security measures to manage the risks introduced by using mobile devices. These measures may include the encryption of mobile devices containing sensitive information.

9.9.2. The UFS must implement appropriate security measures to protect information accessed or processed from remote sites (e.g. via web access or VPN), or stored there. Additionally, all remote desktop access to UFS resources must be recorded/logged and monitored.

9.9.3. Remote access must be restricted to the minimum services and functions required for business purposes.

9.9.4. Remote access must be revoked when the connection is no longer required, i.e. in the event that a staff member's employment is terminated or a user is found to be in breach of an agreement or policy.

9.9.5. Remote access authentication must be performed using strong authentication mechanisms that require users to log on to the domain with their user ID and password.

9.9.6. All network traffic used for remote access connections must be encrypted using approved encryption mechanisms.

9.10. Third-party access

9.10.1. Third-party access must comply with all remote access policies and procedures, where applicable.

9.10.2. In cases where UFS computers or networks are connected to third-party computers or networks, the RMC must have determined that the combined system will be in compliance with UFS security requirements prior to allowing the connection.

9.10.3. Third-party access to the UFS's data processing facilities must be monitored, controlled, documented and approved.

9.10.4. As a condition of gaining access to the UFS network, all third parties must be required to secure their own connected systems in a manner consistent with the university's requirements.

9.10.5. The UFS also reserves the right to immediately terminate network connections with all third-party systems not meeting such requirements.

9.10.6. All third-party accounts must be revoked upon termination of their contract with the UFS.

9.10.7. Third-party access must be governed by formal agreements. The agreements must:

- Require the third party to comply with any necessary security standards and procedures.
- Include a confidentiality clause, where appropriate, to ensure that third-party contractors do not make unauthorised use of UFS information.

9.10.8. Contractors and third parties working on information systems must sign acknowledgement of information security policies.

9.10.9. UFS must regularly monitor, review and audit third-party delivery.

9.11. Network security

9.11.1. The security mechanisms, service levels and management requirements of all network services must be identified and included in service agreements, irrespective of whether these services are provided in-house or outsourced.

9.11.2. All network devices, including wireless access points, must be logically and should be physically secured according to approved procedures.

9.11.3. Wireless networks are considered unsafe when unprotected. They must be deployed with ICT Services-approved encryption and authentication standards.

9.11.4. Network equipment (other than client devices) must only be connected to the network and deployed by ICT Services.

9.11.5. Network points must, as far as possible, be segregated from one another.

9.11.6. All Internet traffic should be logged to identify the computer and/or user.

9.12. Firewall management

9.12.1. Firewalls must be implemented and monitored to protect against attacks or any unauthorised access from external and internal networks. Firewalls must control network traffic flow in both directions.

9.12.2. The following requirements must be met in the management, modification and support of firewall systems at the UFS:

<u>Responsibilities:</u>

9.12.2.1. Segregation between the approval and implementation of firewall changes must be enforced.

9.12.2.2. All modification of existing firewall rules or the creation of new firewall rules must be approved by the OCC.

9.12.2.3. The head of the division responsible for managing the technical configuration of the firewall must ensure that all firewall security-related administrative tasks are implemented and that applicable maintenance is performed, if necessary.

<u>Firewall services:</u>

9.12.2.4. Firewalls are dedicated devices or systems, and under no circumstances must any UFS host operating as a network firewall be configured to provide any other service.

9.12.2.5. Individual hosts must, where possible, use approved local firewall rules as a second layer of protection and must only allow required services to be accessible.

<u>Firewall host:</u>

9.12.2.6. All firewalls must be provisioned by authorised IT infrastructure staff in accordance with documented change management policies and procedures.

9.13. Encryption

9.13.1. Procedures for the use, protection and lifetime of cryptographic keys must be developed and implemented by the UFS throughout their entire lifecycle, which includes the generation, storage, archiving, retrieval, distribution, retiring and destruction of keys.

9.13.2. All sensitive information that is stored or transmitted must be encrypted using approved encryption algorithms.

9.13.3. User authentication credentials are regarded as sensitive information and must be encrypted during transmission.

9.13.4. Certificates used for the encryption of data in transmission, such as SSL certificates, must not be self-signed on systems containing sensitive information or any production system.

9.14. Vulnerability management

9.14.1. A process must be implemented to detect and evaluate the technical vulnerabilities of UFS systems in a timely manner and to ensure appropriate remedial action to address the associated risks. This may be performed through regular vulnerability assessments and penetration tests.

9.14.2. All security patches must be tested prior to installation on hardware, operating systems and software packages. The patches must be kept current and implemented in a controlled manner.

9.14.3. Exceptions must be formally documented in cases where security patches cannot be installed on systems due to compatibility issues. Alternative control measures must be identified and implemented, as far as possible, to mitigate the associated risks.

9.15. Antivirus and malware protection

9.15.1. Detection, prevention and recovery controls to protect against malware must be implemented with appropriate user awareness.

9.15.2. All computers and relevant servers (including the mail servers) must have approved antivirus software installed to provide real-time scanning protection for files and applications.

9.15.3. Antivirus software must be obtained from a proven leading supplier and only approved antivirus software must be installed on laptops and desktop computers.

9.15.4. The antivirus software must be managed and controlled from a central console.

9.15.5. The antivirus solution used should also protect against malware, spyware and other relevant vulnerabilities.

9.15.6. All emails sent to and from the UFS mail servers must be scanned for malware.

9.16. Physical and environmental controls

9.16.1. Physical access points, such as delivery and loading areas and other points where unauthorised persons could enter the UFS premises, must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

9.16.2. Power and telecommunications systems and data carriers transporting UFS data or supporting information services should be protected from interception, interference or damage.

9.16.3. UFS equipment must be correctly maintained to ensure continued availability and integrity of digital infrastructure.

9.16.4. UFS data processing equipment, information or software must not be taken offsite without prior authorisation.

9.16.5. The UFS data centre must be protected by physical security measures that prevent unauthorised access.

9.16.6. The construction of the UFS data centre and recovery site must offer adequate protection against threats such as fire, water damage and vandalism.

9.16.7. Access to the UFS data centre must be controlled. This entails, among other things, proper identification of authorised staff members entering the data centre.

9.16.8. All persons with the exception of authorised data centre staff must sign a register when entering the data centre. Visitors must provide their details, including name and company, date and time, and the reason for the visit. A staff member authorised by the head of the unit responsible for the data centre must accompany a visitor who requires access to the data centre.

9.16.9. Authorised data centre staff must deny entry to unauthorised staff members who want to install or remove equipment without approval.

9.16.10. Authorised data centre staff should perform maintenance/repairs on an as-needed basis, 24 hours per day.

9.16.11. When an authorised data centre staff member resigns, all physical access rights must be removed.

9.16.12. All business-critical systems must be protected by emergency power systems with at least 3 hours of capacity.

9.16.13. UFS equipment must not be removed from the data centre without appropriate authorisation.

9.16.14. Hardware must be marked for identification and inventory control. Inventory records of hardware must be kept current.

9.16.15. ICT Services must define and implement procedures to grant, restrict and revoke access to the ICT Services premises in response to business needs, including emergencies. Access to premises, buildings and areas must be justified, authorised, logged and monitored.

9.16.16. Physical access procedures must apply to all persons entering the premises, including staff, temporary staff, students, vendors, visitors and any other third parties.

9.16.17. Physical security measures must make provision for the effective prevention, detection and mitigation of risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.

9.17. Backups

9.17.1. Information, software and system images must be backed up in accordance with an approved backup procedure that meets the following minimum requirements:

9.17.1.1. Regular full backups must include data and configuration items.

9.17.1.2. Logs of completion and verification of backups must be retained and formally reviewed.

9.17.1.3. ICT Services must provide acceptable schedules for the backup of systems. These schedules must consider appropriate time-frames for backups on weekdays and weekends to minimise disruption to business processes.

9.17.1.4. Periodic testing of backups and other recovery mechanisms must be performed to ensure the continued availability of critical systems, such as ERP systems.

9.17.1.5. The removal of backup media from the alternative storage site as well as their retrieval must be formally recorded. The staff member delivering or collecting backup media must sign a register to ensure accountability.

9.17.1.6. Backups of sensitive, critical or valuable information must be stored offsite in an environmentally and access-controlled site.

9.17.1.7. Backed-up information must be retained in accordance with UFS retention periods, which are based on contractual, legislative, regulatory and business requirements.

9.17.1.8. In the event that data recovery is required from the backup media, stakeholders and operational data stewards must be informed accordingly.

9.17.1.9. Backup media must be encrypted to ensure unauthorised access is not gained to sensitive information.

9.18. Information availability and security continuity

9.18.1. The UFS must determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

9.18.2. The UFS must establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

9.18.3. The UFS must verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

9.18.4. ICT Services must ensure that a written plan is developed, containing at least the following to enable the smooth recovery of critical systems and continuity of operations:

- Business impact analysis.
- Critical information on continuity teams, affected staff, suppliers and public authorities (if required).
- Acceptable alternative sites.
- Emergency support arrangements - documented and formalised.
- Recovery point objectives and recovery time objectives defined.
- Security requirements at alternative sites.
- Emergency supplies and procedures to ensure safety of all affected members.
- Post-recovery procedures, i.e. recovery procedures meant to bring the business back to the state it was in before the incident or disaster.
- Clear roles and responsibilities for disaster recovery team members.
- Coordination procedures.

9.18.5. Disaster recovery plans must be stored at the offsite facility. Operational data stewards must provide change control procedures in order to ensure that the continuity plan is up to date and reflects actual business requirements. This requires continuity plan maintenance procedures, aligned with change and management and human resources procedures.

9.18.6. Disaster recovery plans should be tested on an annual basis. This may be performed through simulation testing or bringing down specific areas of the system for testing the disaster recovery plan. This requires careful preparation, documentation, reporting of results and implementation of an action plan (based on the results).

9.18.7. Disaster recovery plans, given the sensitive nature of information in the plan, must only be distributed to authorised personnel and must be safeguarded against unauthorised disclosure. Consequently, sections of the plan must be distributed on a need-to-know basis.

9.18.8. UFS information processing facilities must have sufficient redundancy measures in place to meet availability requirements.

9.18.9. Changes to the university, business processes, information processing facilities and systems that affect information security must be controlled.

9.18.10. The use of UFS resources must be monitored and projections should be made of future capacity requirements to ensure the required system performance.

9.19. Server management and configuration

9.19.1. ICT Services must create, approve and maintain server configuration guides for each operational group, based on business needs.

9.19.2. Servers must be registered on the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact.
- Hardware and operating system.
- Main functions and applications.
- Service severity classification.

9.19.3. Configuration changes made to production servers must adhere to the approved change management procedures.

9.19.4. Configuration of operating systems must be performed in accordance with the approved ICT Services guidelines.

9.19.5. Services and applications that are not used should be disabled, wherever practical.

9.19.6. The use of trust relationships between systems poses a security risk and should be avoided, wherever possible.

9.20. Information asset management

9.20.1. Operational data stewards must identify assets associated with information and information processing facilities and an inventory of these assets must be drawn up and maintained.

9.20.2. Each information asset must be assigned an operational data steward and/or data governor.

9.20.3. Rules for the acceptable use of UFS information and assets associated with UFS information and information processing facilities must be identified, documented and implemented.

9.20.4. Operational data stewards must classify all UFS information in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

9.20.5. Procedures for the labelling and handling of information assets must be developed and implemented in accordance with the information classification scheme adopted by the UFS.

9.20.6. Procedures for the management of removable media must be implemented in accordance with the classification scheme adopted by the UFS.

9.20.7. Information on mobile devices like notebooks, external hard drives and memory sticks must be encrypted. Key code-protected memory sticks must be used to safeguard information if it is not encrypted.

9.20.8. Media must be disposed of securely when no longer required, using formal procedures.

9.20.9. Media containing UFS information must be protected against unauthorised access, misuse or corruption during transportation.

9.21. Software installation and monitoring

9.21.1. ICT Services must establish and implement procedures to control the installation of software on production systems.

9.21.2. ICT Services must establish and implement rules to control the installation of software by users.

9.21.3. All software deployed on UFS systems must be under security patch support.

9.21.4. Deployment and utilisation of software must be compliant with the software license agreement of the vendor and relevant legislation.

9.22. System acquisition, development and maintenance

9.22.1. The UFS must address information security as part of project management, regardless of the type of project.

9.22.2. Information security-related requirements must be included in the requirements for new information systems or enhancements to existing information systems.

9.22.3. UFS information transmitted via public networks (such as the Internet) must be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.

9.22.4. UFS information involved in service transactions must as far as possible be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

9.22.5. Rules for the development of UFS software and systems must be established and applied to developments at the university.

9.22.6. Changes to systems within the UFS development lifecycle must be controlled by the use of formal change control procedures.

9.22.7. When operating platforms are changed, business critical applications must be reviewed and tested to ensure there is no adverse impact on UFS operations or security.

9.22.8. Modifications to software packages must be discouraged, limited to necessary changes and strictly controlled.

9.22.9. The UFS must establish and appropriately protect secure development environments for system development and integration efforts, covering the entire system development lifecycle.

9.22.10. UFS must review and monitor outsourced system development activities.

9.22.11. Testing of security functionality must be carried out during development.

9.22.12. Acceptance testing programs and related criteria must be established for new information systems, upgrades and new versions.

9.22.13. UFS production data used for testing purposes must be carefully selected, protected and controlled. Personal information should be anonymised on test and development systems.

9.23. Compliance and internal control

9.23.1. All legislative, statutory, regulatory and contractual requirements relevant to the UFS as well as the UFS's approach towards meeting these requirements must be explicitly identified, documented and kept up to date.

9.23.2. Relevant legislation includes, but is not limited to:

- Public Finance Management Act (PFMA), 1999.
- Electronic Communications and Transactions Act (ECTA), 2002.
- Protection of State Information Act, 1982.
- Promotion of Access to Information Act (PAIA), 2000.
- Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA), 2002.
- Basic Conditions of Employment Act, 1997.
- Protection of Personal Information Act (POPIA), 2013.

9.23.3. Appropriate procedures must be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software products.

9.23.4. UFS records must be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislative, regulatory, contractual and business requirements.

9.23.5. Privacy and protection of personally identifiable information, as identified and classified by the UFS, must be ensured as required by the relevant legislation and regulation.

9.23.6. Cryptographic controls, such as encryption, must be used in compliance with all relevant agreements, legislation and regulations.

9.23.7. The UFS's approach to managing information security and the implementation thereof (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.

9.23.8. Operational data stewards must at least annually review the compliance of information processing as well as procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

9.23.9. All critical information systems must be periodically reviewed for compliance with UFS information security policies and standards.

9.23.10. University-wide audits should be performed by Internal Audit and appointed external auditors. As a result of audits, corrective actions may be suggested and presented to the management of the affected units.

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 abovementioned resources.

12. Review procedure

12.1. The policy must be reviewed on at least an annual basis, 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 may include:

- New threats or risks associated with UFS information resources.
- Information security incidents.

- Changes to information security requirements or responsibilities (new government regulations, new roles defined in the institution, new or modified security controls implemented, etc.).
- Changes to the university's organisational or technical infrastructure that impact information resources (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 have been 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 Data Governors and Data Stewards
Document number	IS 1001
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 • Information Security Policy for Users of Information