University of South Australia

Information Security Policy

Responsible Officer:	Chief Information Officer
Last Updated:	May 2020
Date of Review:	May 2023
Audience/Application:	Staff
Related Documents	– Acceptable Use of Information Technology (C-22) – Confidentiality of Students Personal Information (A-46) – Risk Management (C-24) – Information Security Policy – Appendix A – Guideline for Off Campus Computing Models

1. PURPOSE AND SCOPE

The purpose of this policy is to ensure that the University's information systems are recognised as a valuable asset and are managed accordingly to ensure their integrity, security and availability. This policy applies to all users of the University's information systems, including those who install, develop, maintain, and administer those information systems.

The purpose of this policy is to ensure:

- The provision of reliable and uninterrupted information systems;
- The integrity and validity of data contained in information systems;
- An ability to recover effectively and efficiently from disruption to information systems; and
- The protection of the University's IT assets including information, software and hardware.

Within this policy information assets (e.g. databases, files); software assets (e.g. applications and systems software and development tools); and hardware assets (e.g. computers, communications equipment and magnetic media) refer to those assets which taken together comprise the University's information systems.

All users of the University's information systems should be aware of their responsibilities as described in the Acceptable Use of Information Technology (C-22)

2. RISK ASSESSMENT

The University will carry our regular risk assessments of its information systems using the University's risk management procedures. These risk assessments will examine potential vulnerabilities and security measures and will lead to the development of controls consistent with reducing the identified risk to an acceptable level. Refer to the University policy on Risk Management (C-24).

Information systems hosted off campus must comply with the University's guidelines for Off Campus Computing Models. These guidelines require the preparation and approval of a detailed risk assessment by the relevant System Owner.

3. ACCESS MANAGEMENT

All users must be authorised to access the University's information systems by the relevant system owner. System owners are as identified in the University's Major ICT Incident Response plan. Access is controlled and monitored in accordance with University policy.

3.1 Identification

All information system users are granted a unique ID. This unique ID is to be used to access the University's information systems and where relevant external information technology systems operated by third party providers. User IDs are not to be shared. Users are responsible for maintaining the security of their IDs and all activity occurring under those IDs. IDs are issued in accordance with approved standards. In special circumstances, temporary generic accounts may be approved by the Chief Information Officer or delegate.

3.2 Authorisation

Only those users who have valid reasons (as determined by System Owners) for accessing the University's information systems are granted access privileges appropriate to their requirements. Access is granted by means of a computer account, which also serves as identification. Accounts are issued in accordance with approved standards.

Users who have access to multiple critical roles (where segregation is not enforced), should have their use regularly reviewed to ensure their use is appropriate. Particular focus should be given to the use of these roles in periods where that level of access may not be required.

3.3 Authentication

Authentication ensures an identity. Each ID requires a technique, usually a password, for validating identity. Standards apply to all systems requiring authentication.

3.4 Account Management

All System Owners must regularly review their schedule of delegated authority, to determine who is authorised to use the system and their level of authorisation.

At a minimum, an annual review of all system access levels of users should be carried out. System Owners should ensure any non-compliance as a result of this activity is addressed as a matter of priority. All records of non-compliance must be kept until all matters arising from non-compliance have been resolved.

3.5 Privileged Users

System administrators have high-level access rights, enabling them to access any data stored on the University's information systems. System administrators should abide by the Code of Ethics promulgated by the System Administrators Guild of Australia and should sign a confidentiality agreement on at least an annual basis. System Administrators found guilty of breaching this Code of Ethics may be subject to disciplinary action as recommended by the Chief Information Officer.

Contractor and third-party access are permitted only if agreed to by the System Owner and a full-time employee sponsors the individual. These parties must comply with access control standards which require, at a minimum, that a unique user ID identify each user. All temporary accounts should have an expiration date based on contract completion date.

3.6 Information Systems Operated by Third Parties

Users who use their unique ID and password to access information systems and resources operated by third parties must ensure they comply with the applicable Information Security and Acceptable Use policies applying to those systems and resources.

4. ASSET SECURITY MANAGEMENT

All major information systems must have a nominated owner who is responsible for the implementation and management of this policy in relation to those assets.

4.1 Server and System Backup

All critical University information should be stored on professionally maintained networked disc storage and must be backed and/or journaled up on a regular basis. Frequency of backup is determined by the frequency with which the data changes and the effort required to recreate the information if lost. Standards apply to the backup of data from all University systems.

Data stored in other locations (eg. on servers, desktops, laptops and other mobile devices) becomes the responsibility of the user to ensure it is backed up on a regular basis.

4.2 Recovery

All backups of critical data must be tested periodically to ensure that they support full system recovery. System Administrators must document all restore procedures and test these on a regular basis, at least annually. Backup media must be retrievable within 24 hours, 365 days a year. Standards apply to the recovery of data from all University systems.

4.3 Off-Site Storage (Backup Media)

Off-site storage locations must provide evidence of adequate fire and theft protection and environmental controls. A formal Service Level Agreement (SLA) must exist with the off-site storage provider and a site visit should be undertaken on an annual basis.

4.4 Data Retention

Owners of University data are responsible for defining and documenting the length of time data must be retained. The retention period, legal requirements, responsible parties, and source of legal requirement should be specified. System Administrators are responsible for ensuring that these documented requirements are adhered to.

4.5 Business Continuity and Disaster Recovery

As part of the University's Risk Management Framework, Business Continuity and Disaster Recovery Plans should be prepared and tested for all of the University's major systems. The testing strategy to be implemented will be influenced by the importance of the system to the University's business operations and the ability to recover the system within agreed timeframes.

4.6 Physical Security

Access to secure areas, including computer rooms, network equipment rooms and any associated service facilities, is restricted to authorised University staff. All wiring closets must be secured to prevent any damage and to stop unauthorised attempts to connect to data outlets.

4.7 Information Classification

Information assets are classified into four categories: Public, Internal, Confidential and Restricted. All major information assets must have a nominated owner who is responsible for establishing authentication and authorisation procedures commensurate with these categories noting that:

- Public information can generally be made available or distributed to the general public. This is information which does not require protection and when used as intended would have little to no adverse effect on the operations, assets or reputation of the University or the University's obligations concerning information privacy.

  Examples of public information include:
  - University marketing or promotional information
  - Program and course information
  - Student support information (FAQ's, campus maps)
  - Published research.

- Internal information is for general internal University use only and not for external distribution (internal information may be accessed by authorised staff and students).

  Examples of internal information include:
  - Learning and teaching resources
  - Lecture materials
  - Lecture recordings
  - Library databases and journals,
  - Non-public University policies,
  - De-identified data sets including clinical research

- Confidential information is for internal use only with access only by staff who require it in the course of performing their University responsibilities (confidential information includes information that is protected by Federal and/or State legislation or business contractual obligations) and requires privacy and security protections.

  Examples of confidential information include:
  - Procurement documentation
  - Commercial contracts
  - Financial and billing information
  - Intellectual property
  - Information and physical security logs
  - Personally identifiable sensitive information
  - Credit/debit card details
  - Disciplinary information
  - Individual salary information
  - Completed examination papers
  - Performance Management evaluations
  - Student academic records
  - Commercially sensitive research
  - Commercially sensitive audit reports.
  - Critical infrastructure information (physical plant detail, IT systems information, system passwords, information security plans, etc.)

- Restricted information which is to be kept strictly confidential with access on a strictly "needs to know" basis. Examples include information affecting national interests and/or national security.

Staff should be aware of their legal and corporate responsibilities concerning inappropriate use, sharing or releasing of information to another party. Any third party receiving confidential or restricted information must be authorised to do so

and that individual or their organisation should have adopted information security measures, which guarantee confidentiality and integrity of that data.

4.8 Information Labelling

Wherever practicable information assets should be labelled as follows:

Classification	Labelling
Public	None required
Internal	None required
Confidential	X-in-Confidence (where X = one of Security, Staff, Commercial, Medical, Legal, Council, or Student)
Restricted	Restricted

4.9 Handling and Distribution of Information Assets

The following restrictions apply to the handling of information assets.

Public Information

There are no specific restrictions on the distribution or handling of public information, although University personnel must respect all copyright, trademark and intellectual property rights of any information or data that they distribute.

Internal Information

Internal information is considered non-public and should be protected from unnecessary exposure to parties outside of the University.

- **Access**: University employees, or non-employees with signed nondisclosure agreements, who have a legitimate business or academic need to know.
- **Distribution within the University**: Information can be shared via the web, but the user must provide University authentication, or a federated authentication.
  Electronic and hard copy information can be circulated on a need-to-know basis to University members subject to applicable laws (e.g. copyright) and University Policies.
  Internal information may be accessed remotely and via disk-encrypted portable and mobile devices without further encryption
- **Distribution outside the University**: Information can be sent in unencrypted format via University email to external parties on a need to know basis. Information can be shared using University IT facilities e.g. OneDrive, SharePoint, shared file servers.
  Information circulated via the University internal email system.
- **Storage**: Must be stored using University provided facilities.

- **Disposal/Destruction**: Electronic data should be securely and reliably erased or media physically destroyed.

Confidential information

Confidential information should be protected to prevent unauthorized access or exposure.

- **Access**: University employees whose job function requires them to have and are approved by their supervisors and System Owners to have access, and University vendors or consultants who have executed non-disclosure agreements with the University.
- **Distribution within the University**: Access to confidential data must be strictly controlled by the System Owner who should conduct regular access reviews. Confidential information may be shared with authorised users via University IT facilities, including remote access, subject to University authentication. Encryption of data must be used for all web based access to confidential information. Confidential data must not be extracted from University IT systems and stored on local IT systems without previous approval from System Owners.
  If a portable device (e.g. a laptop, tablet or phone) is used to access University confidential information, the device must be encrypted and require a password or PIN to access.
- **Distribution outside of the University**: Electronic files must be encrypted (and optionally signed) using a public key encryption algorithm or be password protected at the application level (i.e. signed PDF or Word document.) The encrypted/ password-protected files can then be sent via email and/or secure electronic file transmission. Third parties who are handling and/or storing confidential information must agree to abide by the University's policies for safeguarding such information.
- **Storage**: Information must be stored using University IT facilities. Portable devices must have full disk encryption. Unencrypted removable media (e.g. USB sticks or drives) must not be used. Encrypted removable media are not permitted without undertaking evaluation of other options by IT Support Staff. Storage on Personally owned (e.g. home) computer is NOT permitted.
- **Disposal/Destruction:** Electronic data should be expunged/cleared with a data scrubbing utility to ensure that portions of the original data cannot be reconstructed from the hard drive or other electronic storage medium.

Restricted Information

Restricted information has the highest level of sensitivity and represents the most risk to the University, the State, and individuals should such information be accessed by or exposed to unauthorized parties. Therefore, University employees

who handle Restricted Information or who use systems that store, transmit, or manipulate Restricted Information are required to maintain the confidentiality, integrity and availability of such information/data at all times.

The access, distribution, storage and disposal of Restricted information may be subject to applicable State and Federal legislation and will require approval and review of the Chief Information Officer.

4.10 Software Security

Software for the purpose of this policy document is defined as the programs and other operating information used by, installed on, or stored on University owned computer systems or storage media (such as DVDs, CDs, backup tapes).

System Owners and System Administrators must ensure that software and other applicable materials are licensed (as required) in an appropriate manner.

All software, including patches, upgrades or new versions, should be tested, archived and documented before being put into production. This transition should be completed under change management procedures. Control measures should also be in place for maintaining and accessing program and system source libraries.

All operational software should be maintained at current versions or at a level supported by the supplier. In special circumstances, a non-current version of software for a legacy system may be retained for compliance purposes. Processes should also be in place to ensure that information systems development and operational environments for critical systems are separated logically from each other.

Security controls of audit trails and activity logs for the validation of data and internal processing are to be built into applications developed by the University.

4.11 Internet Security

Computer devices connected to the Internet face significant risk of unauthorised access, or inappropriate use. A number of measures should be taken to mitigate this risk. Standards apply to all Internet capable devices requiring protection.

4.12 Email Security

Unsolicited email can affect the performance of the email delivery system and the productivity of the user. To reduce the level of unsolicited messages, email that meets one or more of the following criteria will be blocked or rejected:

- Malformed email
- Email with an attachment identified as a significant risk
- Email that exhibits a significant level of unsolicited email characteristics.

4.13 University Provided End-user Computing Device Security

All University provided end-user computing devices including workstations, laptops, tablets and smart phones which connect to the University network will be configured, wherever possible to use:

- the University licensed anti-virus software with automatic definition update to ensure that the device is protected from known malicious code;
- automated patching process to ensure that operating systems and applications are kept up to date; and;
- device timeouts and password/PINs/biometric setting to minimize the risk of unauthorised access to the device.

By default, users will not have administrative access to their device but may be granted such access in special cases. The installation of software and changes to the device's configuration should be performed with the assistance of IT support staff.

Users must diligently protect mobile computing or storage devices from loss or disclosure of private information belonging to or maintained by the University.

Confidential data must not be downloaded to mobile or offsite computing devices, or storage devices unless approval has been obtained from the relevant data owner.

Mobile computing or storage devices that contain confidential University information must use encryption or equally strong measures to protect the data while it is being stored. Individual folders can be encrypted using instructions provided in AskIT (search for encryption).

4.14 Personally Owned[1] Device Security

This section applies to personally owned computing and storage devices which store any Internal or Confidential data related to the University such as University email, contacts and data in cloud storage.

Users must diligently protect mobile computing or storage devices from loss or disclosure of private information belonging to or maintained by the University.

Users must not store University data on personally owned devices or any other device not owned by the University where such device can be used by another person, unless such devices are locked down to the staff member via password, pin or biometric access and the device locks itself after no more than 5 minutes of inactivity.

[1] Personally Owned Devices means devices owned personally by the staff member or a third party.

Confidential data must not be downloaded to personally owned computing or storage devices unless approval has been obtained from the relevant data owner.

Personally owned computing or storage devices that contain confidential University information must use encryption or equally strong measures to protect the data while it is being stored.

Restricted information must not be stored on a personally owned device.

5. SECURITY INCIDENT NOTIFICATION & REPORTING

5.1 Security Incidents

A security incident is defined as any action or event in contravention of the provisions of this Information Security Policy; actions or events that contravene the provisions of policy established by organisations of which UniSA is a member (eg. AUSCERT, AARNet); and/or actions or events deemed a security incident or breach by State or Federal Police organisations.

5.2 Notification of a Security Incident

Once an incident is confirmed, the responsible officer should take these steps as urgently as possible.

a) The Chief Information Officer should be notified immediately. The University may disable accounts without notice, regardless of whether the account itself is suspected of having been misused.

b) If the security incident involves a possible breach of State, Federal or International law, then the Chief Information Officer or delegate will notify the South Australian Police Service or Australian Federal Police (as appropriate), as soon as is practicable.

c) If another department of the University is involved, then that department should be notified as soon as possible, preferably via the Unit Director or Executive Dean.

d) If an organisation or person external to the University is involved in any capacity, then the Australian Computer Emergency Response Team (AUSCERT) should be contacted.

e) If an organisation or person external to the University is involved as a potential victim, then that organisation or person should be advised as soon as possible.

5.3 Reporting a Security Incident

The person authorised by the Chief Information Officer, to carry out the technical investigation of a security breach must adhere to the process detailed in the Security Incident Management guide. A report of the incident should be prepared for the Chief Information Officer. Once approved, the report should be submitted to the relevant Unit Director or Executive Dean outlining the following details (where possible):

1) General nature of the security incident;
2) General classification of people involved in the security incident, (such as external client, privileged staff member);
3) Computer systems involved in the security incident;
4) Details of the security incident;
5) Impact of the security incident;
6) Possible courses of action to prevent a repetition of the security incident.

Where appropriate, the relevant Unit Director or Executive Dean should undertake remedial action on the basis of this report. Where a significant IT risk is identified the Chief Information Officer is responsible for undertaking a risk assessment as part of the University's Risk Management Plan.

5.4 Unauthorised Access Attempts

All unauthorised access attempts must be logged. The Audit Trail/System Access Log must be reviewed regularly, exception reports generated and inspected by the System Administrator and appropriate action taken. A copy of the report of unauthorised access attempts must be produced and kept for future reference.

6. INFORMATION SECURITY RESPONSIBILITIES

6.1 Chief Information Officer

The Chief Information Officer is responsible for:

- Providing appropriate security of the University's central information technology facilities including ensuring relevant security standards and responsibilities are delegated, developed and implemented;
- Providing oversight of IT security across the University;
- Providing specialist information security advice to the Vice Chancellor and other senior officials of the University;
- Receiving reports of incidents, threats and malfunction that may have an impact on the University's information systems;
- Ensuring remedial action is taken on all reported security breaches;
- Acting as the University's representative on external bodies, including law enforcement agencies, on matters relating to IT security; and
- Implementing disciplinary action for inappropriate use as delegated by the relevant University policies.

6.2 Manager: Cyber Security

The Manager: Cyber Security is responsible for managing information security standards, procedures and controls intended to minimise the risk of loss, damage

or misuse of the University's information technology resources. More specifically, the Manager: Cyber Security's responsibilities include:

- Developing and maintaining the University's Information Security Policy;
- Establishing and maintaining high-level standards and related procedures for access to the University's information and systems;
- Selecting, implementing and administering controls and procedures to manage information security risks;
- Distributing security report information in a timely manner to Chief Information Officer and other appropriate University administrators;
- Liaising with external security authorities (e.g. AUScert, State and Federal Police); and
- Promoting security awareness within the broader University community.

6.3 System Owners

System owners have the authority to make decisions related to the development, maintenance, operation of and access to the application and data associated with that business activity. More specifically, the System Owner's responsibilities include:

- Interpreting relevant laws and University policies to classify data and define its level of sensitivity;
- Defining required levels of security, including those for data transmission;
- Developing guidelines for requesting access;
- Reviewing and authorising access requests;
- Establishing measures to ensure data integrity for access to data;
- Reviewing access by users with critical roles particularly when segregation of duties cannot be implemented;
- Reviewing usage information;
- Defining criteria for archiving data, to satisfy retention requirements; and
- Developing and testing business continuity plans.

6.4 System Administrators

A System Administrator must take reasonable action to assure the authorised use and security of data during storage, transmission and use. A System Administrator is responsible for:

- Developing, maintaining and documenting operational procedures to include data integrity, authentication, recovery, and continuity of operations;
- Ensuring that access to data and applications is secured as defined by the System Owner;
- Providing adequate operational controls to ensure data protection;

- Ensuring that access requests are authorised;
- Modifying access when employees terminate or transfer;
- Communicating appropriate use and consequences of misuse to users who access the system;
- Protecting confidential files and access control files from unauthorised activity;
- Performing day to day security administration;
- Taking remedial action in respect of all audit findings and reported security breaches;
- Maintaining access and audit records;
- Creating, distributing and following up on security violation reports; and
- Developing and testing disaster recovery plans.

System Administrators should be properly trained in all aspects of system security.

6.5 Unit Director/Executive Dean (or equivalent)

A Unit Director/Executive Dean (or equivalent) is responsible for ensuring that security policy is implemented within their area of responsibility. These duties may be delegated; however, it is the responsibility of the Unit Director/Executive Dean (or equivalent) to:

- Ensure that employees understand security policies, procedures and responsibilities;
- Approve appropriate data access;
- Review, evaluate and respond to all security violations reported against staff and students and take appropriate action; and
- Communicate to appropriate University areas when employee departures and changes affect computer access.

6.6 University's Internal Audit Office

Assurance Services is responsible for providing an independent assessment on the adequacy of security procedures within the IT infrastructure and information systems.

Assurance Services is also responsible for evaluating information security policy and procedures compliance during regular operational audits of the University's information systems.

6.7 Users

Users of the University's Information Technology Resources are responsible for:

- keeping their password secure and ensuring it is not shared with any other user;

- ensuring the security of their workstation by logging off or locking it when it is left unattended;
- ensuring the safe keeping of data within their own area of work within any systems they have been granted access to;
- storing and labelling data appropriately, and
- reporting security incidents or problems as soon as possible to the IT Help Desk.

7. COMPLIANCE

The University considers any breach of security to be a serious offence and reserves the right to copy and examine files or information resident on or transmitted via the University's information technology resources. Breaches by staff or students that constitute misconduct will be addressed by the relevant staff or student disciplinary procedures. See Appendix A of the Appropriate Use of IT Facilities (C-22).

Information Strategy and Technology Services may confiscate computer equipment; temporarily remove material from websites or close any account that is endangering the running of the system or that is being reviewed for inappropriate or illegal use.

8. AWARENESS AND COMMUNICATION

It is essential that all aspects of information security, including confidentiality, privacy and procedures relating to system access, are incorporated into formal staff induction procedures and conveyed to existing staff on a regular basis.

Each employee, on commencement of employment, should be made aware that they must not divulge any information that they may have access to in the normal course of their employment. Staff must also be made aware that they should not seek access to data that is not required as part of their normal duties.

Students must be informed at initial enrolment and from time to time of their information security responsibilities.

9. ACKNOWLEDGEMENT

This policy is based largely on the Griffith University Information Security Policy.