IT SECURITY PROCEDURES

These Procedures are made under the IT Acceptable Use and Security Policy, to support the principles enunciated in that Policy by:

a) Establishing clear responsibilities of University IT Custodians, including Technology Services.
b) Establishing requirements for technical controls to protect the security of information assets.

Definitions

PCI-DSS (payment card industry data security standard) is a security standard set out by PCI that must be implemented for organisations accepting payments using credit cards.

Class 3 data refers to University data that is classified as Class 3 under the University's Information Classification and Handling Guideline (i.e. there would be serious consequences to the University if security of the data were compromised).

University data means data generated by or on behalf of the University or otherwise within the University's custody.

All other defined terms have the same definitions as used in the IT Acceptable Use and Security Policy.

1. IT Security Governance

Responsibility: University IT Custodians

a) The University must manage its IT in such a way that minimises the risk:
    i. of unauthorised and unacceptable use of University IT,
    ii. to the University and Users of wilful, malicious damage or any activity undertaken to purposely bypass security controls on University IT facilities, and
    iii. to the University and Users of virus infection and malicious software.
b) The University must manage its IT in such a way that electronic data is;
    i. accurate, complete and consistent with University data standards,
    ii. available to be accessed by authorised users, and only those users, when required, and
    iii. able to be recovered as soon as practicable in the event of serious IT systems failures or disasters.
c) In order to achieve the security of University IT:
    i. University IT Custodians must implement security measures consistently using a risk-based approach.
    ii. Technology Services will implement an information security management system (ISMS) that aligns with the international standard ISO/IEC 27001 and ISO/IEC 27002.
    iii. Business Owners must implement security controls as required by the ISMS or as advised by TS.

2. Data Security

Responsibility: University IT Custodians

a) University IT Custodians must implement security controls to protect the security of information in accordance with the University's Information Classification and Handling Guideline.
b) Where credit card information is handled on University IT, University IT Custodians must implement security controls in accordance with the PCI-DSS compliance guidelines issued

by Financial Services (refer to https://www.adelaide.edu.au/finance/fin-services/pci-compliance/).

3. Acquisitions and Change Management

Responsibility: Executive Manager, Branch Head or Head of School

a) Acquisition or development of University IT, including implementation of commercial off-the shelf (COTS) solutions, purchase of hardware and software, development of an IT application, use of third-party hosted ("cloud" or "SaaS") solutions must be done in such a way that it:
   i. meets business requirements;
   ii. aligns with current University architectural strategy;
   iii. integrates with and does not duplicate existing investments;
   iv. does not expose the University to unacceptable levels of information security risk;
   v. is compliant with other University policies (including but not limited to the Contracts and Agreements Policy, Strategic Procurement Procedures and the Disability Action Plan) as well as laws and regulations.

b) Any major changes or upgrades to existing University IT, regardless of whether it is managed by Technology Services or otherwise, must be managed using the Technology Services Change Management framework.

c) In particular, changes that have interdependencies with other systems, or that may have impact on the wider University community, should be coordinated and approved through the Technology Services Change Advisory Board (CAB).

d) University IT that includes presence on the public internet that will be branded as, and/or recognised as, part of the University must undergo a review and approval by Marketing and Communications before go-live.

e) Where University data is to be hosted or stored by a third party vendor, the Third Party Hosting Security Guideline must be followed.

4. Accounts and Access Management

Responsibility: University IT Custodians

a) Technology Services (TS) will provision and de-provision University of Adelaide User IDs based on the Identity Management procedures and business rules defined by Human Resources and Student Services.

b) University of Adelaide User IDs are established by means of a unique logon user ID and protected by a password that meets the current guideline published on the Technology Services website. In particular, passwords must be changed on a periodic basis, and systems must be configured to lock accounts automatically after repeated unsuccessful login attempts.

c) Access to University IT must be granted on the principle of least privilege with minimum access level required for performing the work by a staff, student, or visitor.

d) Heads of Schools and Branch Heads must notify IT Custodians of any changes to access requirements as the result of an account holder's change in role and/or responsibility or termination of employment. IT Custodians must modify access rights for that account holder as soon as possible to be commensurate with the new role and responsibility.

e) Heads of Schools and Branch Heads must notify IT Custodians of any changes to access requirements as the result of change in role and/or responsibility or termination of employment.

f) University IT Custodians must ensure that access to University IT (other than via University of Adelaide User IDs) is protected by unique user name and password.

g) While individual accounts must be used to enable accountability of actions, generic accounts may be required and created from time to time. Generic accounts must have a nominated owner.

h) Head of School or Branch Head must approve creation of generic accounts.
i) Use of generic accounts should be avoided to ensure accountability of actions taken from an account, but may be permitted for shared mailboxes.

Responsibility: Executive Manager, Branch Head or Head of School

j) If a staff member, visitor or titleholder requires a level of access different to that usually given to people in their relevant area, their Head of School or Branch Head must authorise the level of access required and submit that approval to Technology Services.
k) The relevant Branch Head or Head of School must notify TS when visitors who are IT account holders cease their relationship with the University prior to the original contract end date or the termination date as requested on the visitor account request form.
l) If a visitor's relationship with the University changes but does not end, the relevant Branch Head or Head of School must ensure that TS is advised of this change.
m) The access of such visitors to online services and IT facilities will be modified to reflect any changes in their relationship with the University.

5. University Logging and Monitoring

Responsibility: University IT Custodians

a) Custodians of University IT should enable logging of all use of University IT in order to assist in the detection of breaches of this Policy, including unauthorised activities.
b) In addition to routine logging and monitoring, individual account holder's use of University IT will be examined if;
    i. A potential breach of law or University Policy is detected or reported, or
    ii. The University needs to retrieve or examine the content of electronic documents or messages for purposes such as finding lost files or messages, complying with legal authorities, or recovering from system failure, or
    iii. An account holder's Head of School/Branch Head requests that the account holder's use of IT facilities be examined; and that request is deemed reasonable by the Team Leader, IT Risk Management. All information requested will be provided to the requesting Head of School/ Branch Head.
c) The University periodically monitors the content of web pages and may request that nominated material be updated or removed if it is unacceptable.
d) The University will conduct its monitoring and logging of information in accordance with its legal obligations and the Privacy Policy and Management Plan.
e) The University reserves the right to carry out security audits on University IT facilities and services.
f) The University reserves the right to block or filter any network traffic that potentially breaches this policy or is potentially illegal.

6. Disaster Recovery Plan

Responsibility: Executive Managers, Heads of School and Branch Heads

a) Business owners of any critical University IT, in conjunction with their corresponding Custodian, must develop a disaster recovery plan (DRP) that will help to recover services within an acceptable timeframe.
b) DRP should be tested on an annual basis and updated both annually and whenever there is a significant change to the University IT.