University of South Australia

Information Security Policy

Appendix A: Access and Asset Security Standards and Operational Guidelines

Responsible Officer:	Chief Information Officer
Last Updated:	March 2014
Date of Review:	March 2017
Audience/Application:	Staff, Students and External Users
Related Documents	– Acceptable Use of Information Technology (C-22) – Confidentiality of Students Personal Information (A-46) – Risk Management (C-24) – Information Security Policy

1. SCOPE

This document identifies the standards to be applied to access & asset control mechanisms for UniSA's information technology resources and outlines best practice guidelines for operational security management.

2. ACCESS CONTROL STANDARDS

2.1 Identification Standards

IDs will be issued in accordance with the following standards:

- Staff, including casual staff and those on unpaid contracts, on confirmation of appointment and students on acceptance of an offer are provided with unique usernames and passwords;
- Where a user is both a staff member and student then they will be provided with two unique usernames and passwords;
- Any other university approved and authorised users (e.g. visiting scholars) require the relevant Head of School or Business Unit Director to make application for Temporary Network Access (TNA). All TNA usernames and passwords are allocated for a maximum of 3 weeks. If access is required for a longer period visitors must approach their local HR to organise an unpaid contract;
- User IDs are not to be shared. Users are responsible for maintaining the security of their IDs and all activity occurring under those IDs;
- Accounts designed for use by more than one person are not normally permitted. An exception to this can only be authorized by the Chief Information Officer or delegated authority;
- Guest login accounts are not normally permitted. A guest login account will be a temporary account and can only be issued with the approval of Chief Information Officer or delegated authority;
- A maximum of 3 unsuccessful login attempts will be allowed, after which point accounts will be locked. Users will need to contact the IT Help Desk to get their passwords reset. Four points of ID will be required to reset passwords;

- All account creation or system access level requests must have an authorisation application form, from a person empowered (usually Head of School/Business Unit Director) to authorize these types of requests.

2.2 Authorisation Standards

Accounts will be issued in accordance with the following standards:

- Only the authorised user may use an account. A user is authorised to use an account if:
  - The user is the account holder (in the case of a user account); or
  - The account is a public access account; or
  - The user's position within the University implies authorisation and the user has a demonstrated need to use the account to carry out approved activity; or
  - The System Owner believes such authorisation is warranted;
- An account holder will not authorise or allow the use of the account by other persons except where the Chief Information Officer grants permission for the account holder to allow such use of the account. Approval to allow the use of an account by persons other than the authorised account holder must be requested, in writing, from the Chief Information Officer (or delegate) through the relevant Director or Head of School;
- A user will use an account only for approved activities;
- When the System Owner creates accounts for specific public facilities, the University owns these accounts. Users may use them only for the specified purposes;
- The user will not attempt to circumvent the security mechanisms of any computer system unless authorised by the Owner of the computer system. This includes allowing access via unsecured network mechanisms;
- The Chief Information Officer and/or the relevant System Owner may decide to disable or remove accounts if the following events happen:
  - The account is no longer required by the account holder;
  - The account holder ceases to have an association with UniSA;
  - The account is inactive for a given period of time;
  - The account is used for non-approved activities.

2.3 Authentication Standards

The following standards should be applied to all systems requiring authentication:

- Passwords must be used for accessing all corporate systems;
- Passwords must be at least six characters in length;
- Users are encouraged to choose strong passwords. If strong passwords are chosen then there is no need to change them on a regular basis. The University will therefore not force password aging for staff and student accounts except in response, where appropriate to a system change or a security incident;

- The password change application must not allow the use of the four previous passwords;
- Passwords must not be displayed in writing next to the terminal;
- When logging on, users shall take precautions to ensure others do not see their password;
- Passwords must not be disclosed to others;
- Passwords must not be easily associated with a particular user;
- Users must not save passwords electronically within applications except when saved in mobile devices;
- A user who suspects that a password has been compromised must change the password immediately. The user is required to report all details of the suspected breach to the IT Help Desk;
- The use of automatic logons is not permitted with the exception of System Administrators operating in secure mode.

Passwords are automatically checked to ensure that they comply with above standards and are non-trivial. Information on correct selection of passwords shall be readily available and widely distributed. Where possible, all passwords should be stored in an encrypted format on systems.

3. ASSET SECURITY STANDARDS

3.1 Internet Security Standards

The following are the minimum accepted standards for protection of Internet capable devices operating on the UniSA network:

- A firewall, or equivalent, will be used on all systems containing content not of a public nature;
- All data packets and connection requests will be controlled by the firewall, or equivalent;
- Only explicitly permitted traffic is allowed through the firewall, or equivalent. All other traffic is rejected;
- All traffic passing through the firewall must be capable of being captured, logged and audited;
- Where possible, traffic passing through the firewall must be capable of being encrypted;
- Packet filtering will be used with rules which keep the security risk to a minimum;
- All Internet/Web servers which require connectivity to the UniSA network must be approved by the Chief Information Officer or designate;
- All Internet/Web servers will have non-necessary services disabled;
- All Internet/Web servers will be configured to allow access to and use of services to be controlled (e.g. Access Control Lists, TCP Wrappers); and

- Use will be for university-related and approved purposes.

3.2 E-mail Security Standards

The following are the minimum acceptable standards for the use and management of e-mail within the university's information management and technology environment:

- A password must be used on all e-mail systems;
- The use of scanned signatures should be discouraged;
- Make users aware that e-mail communication is not private. Any e-mail that is non-business related should have a disclaimer that the opinions are individual's and not those of the University;
- E-mail systems should be backed up and maintained in accordance with backup and recovery standards;

3.3 Backup and Recovery Standards

The following are the minimum acceptable standards for backup and recovery of the University's information resources:

- Backup cycles should be related to the business risk, frequency with which data and software is changed and criticality of the system to business operations;
- A register of backups, including verification of their success, should be maintained;
- A cycle of backup media should be used for all backups, with at least one copy of each cycle stored off-site;
- In addition to above, a system backup should be performed before and after major changes to either the operating system, system software or applications;
- In some instances, files may be backed up from one disc to another disc. This would be acceptable if the target disc was not in the same location. If the discs are in the same location, backup of critical data should also be performed to other portable media (such as tape) for off-site storage;
- Consideration should be taken when upgrading backup technologies to ensure that backup data is able to be read in the new environment;
- Regular tests of key corporate systems backup data should be performed (in a safe environment) to verify that the system can be recovered from the backups produced;
- A cycle of backup media should be retained of all information required to meet customer service, legal or statutory obligations;
- Operator logs should be maintained, monitored and reviewed on a regular basis to ensure that correct computer operating procedures have been complied with.

4. OPERATIONAL SECURITY GUIDELINES

4.1 Documentation Operating Procedures

When documenting operating procedures and processes, consideration should be given to the following:

- User manuals should be maintained on all current hardware, software applications and in-house developed systems;
- Authorisation processes for approving all changes to corporate information facilities including operating systems, software applications and hardware should be in place;
- Procedures should be in place for recording and monitoring of security violations and exposures.

4.2 Change Control

To minimise threats to operational environments, consideration should be given to the following:

- Operational environment is under change control and any changes are subject to the Request for Change (RFC) process;
- Ensuring adequate testing and change control mechanisms are in place for the migration of new or modified systems into the operational environment;
- Ensuring that the information environment is managed so that future expansions or changes can be accommodated and do not adversely impact the operational environment.

4.3 Malicious Software

There are many types of malicious software that can severely impact information systems, data and networks and undermine the integrity, confidentiality and availability of information.

To minimise threats to the university's operational environment, consideration should be given to the following activities:

4.3.1 Virus Detection and Scanning

- All operational computer equipment should have the current version of anti-virus software installed;
- While server scans should be run on a daily basis, anti-virus software should be configured in "real-time" mode to ensure any infections are identified and cleaned immediately upon detection;
- Anti-virus software should be regularly updated with new definition files;
- All incoming and outgoing e-mail attachments should be scanned. If a virus is detected, the attachment should be cleaned before distribution. If not, then the message and attachment should be blocked and the sender notified;

- Anti-virus software should be regularly reviewed, as it may be necessary to use more than one type of scanning software to ensure that maximum protection is provided for all information platforms and environments;
- To improve security and productivity, the university's email systems should provide the functionality to block unwanted email and SPAM.

4.3.2 Education and Awareness

- Regular communication should be sent to users alerting them of potential virus attacks. Users should be educated about malicious software in general, the risks that it poses, virus symptoms and warning signs including what processes should be followed in case of a suspected virus;
- Users must be made aware that the installation and use of unauthorised software on university owned assets is prohibited.

4.4 Audit

Regular auditing procedures will be carried out on UniSA's information technology resources. The depth and regularity of each level of audit will be part of the University's audit and risk management process.

Regular internal and external vulnerability scanning will be undertaken to identify vulnerabilities. The Chief Information Officer or nominee will be responsible for authorising all vulnerability scanning activity.

4.5 Segregation of Duties

There should be adequate separation of functions and duties where tasks involve activities, which could be susceptible to unauthorised activity, misuse of information or pose a conflict of interest.