Information Security Guidelines

Section 1 - Purpose

(1) Computing and information systems underpin the University's activities and are essential to the teaching, learning, research and administration functions of Charles Sturt University (the University).

(2) The University is a critical education asset under the Security of Critical Infrastructure Act 2018 and subject to mandatory reporting under that Act.

(3) The University acknowledges the requirement to manage cyber risk arising from criminal activities, internal threats, and local and foreign interference.

(4) These guidelines support the Information Technology Policy and set out the University's information security practices regarding the confidentiality, integrity, and availability of all information and communication technology (ICT) infrastructure, systems and processes.

(5) The purpose of these guidelines is to:

a. guide the establishment of appropriate standards, processes, procedures, and guidelines to support the implementation of information security requirements across the University
b. define the University's information security procedure statements and control objectives
c. establish the minimum requirements for effectively managing information security across the University in a risk based manner
d. provide clear direction to authorised users about requirements in protecting the University's information assets from inappropriate use, modification, loss or disclosure, and foreign interference
e. provide a reference to identify, assess and manage areas of non-compliance with the objective of managing risks to the University information assets
f. promote and support the adherence to appropriate legislation, regulation and industry standards and guidelines where applicable, including:
    i. NSW Cyber Security Policy
    ii. Australian Government Information Security Manual (ISM)
    iii. Centre for Internet Security (CIS) Critical Security Controls
    iv. International Organisation for Standardisation (ISO)27000 Series
    v. National Institute of Standards and Technology's Cyber Security Framework (NIST CSF)
    vi. Guidelines to Counter Foreign Interference in the Australian University Sector

(6) Appropriate security standards and measures must be established, implemented, monitored, reviewed and improved as required, to ensure that the University's Information Security Management System (ISMS) documentation framework and business objectives are met.

(7) It is the intent of the University that the Information Security Management System (ISMS) documentation framework be implemented and appropriate security measures are:

a. in place or planned
b. supported by industry guidelines, standards, processes, and procedures to ensure compliance.

Scope

(8) These guidelines apply to all authorised users who own, manage, access or use the University's Information and Communication Technology (ICT) services.

(9) These guidelines cover all:

a. ICT systems and data attached to University networks
b. University systems
c. communications sent to or from the University
d. data owned by the University, either internally or on systems external to the University's network.

References

(10) These guidelines are a component of the University's Information Security Management System (ISMS) documentation framework and should be read in conjunction with, but not limited to:

a. Information Technology Policy
b. Information Technology Procedure - Acceptable Use and Access
c. Information Classification and Handling Procedure
d. Information Technology Procedure - Personal Data Breach
e. Risk Management Policy
f. Privacy Management Plan
g. Records Management Policy
h. Information Technology Procedure - Purchasing and Disposal
i. Australian Government Information Security Manual (ISM)

Section 2 - Policy

(11) See the Information Technology Policy.

Section 3 - Procedure

(12) Nil.

Section 4 - Guidelines

Part A - Organisation of information security

Objective

(13) To establish a management framework for the implementation and operation of information security, and to assign roles and responsibilities for the management of information security within the University.

Information security roles and responsibilities

(14) Information security responsibilities should be defined and allocated in accordance with the Information Technology Policy. Responsibilities for the protection of individual assets and for carrying out specific information security processes should be identified. Responsibilities for information security risk management activities and for acceptance of residual risks are defined in the Information and Communication Technology (ICT) Information Security and Risk Management Policies.

(15) Executive management of the Division of Information Technology have the overall responsibility for information security within the University. Guidelines on roles and responsibilities have been outlined in Appendix B.

Segregation of duties

(16) Roles and areas of responsibility must be segregated to reduce opportunities for unauthorised modification or misuse of information or services. Whenever a computer-based process involves sensitive, valuable, or critical information, the respective system should include controls that ensure that no one individual has exclusive control over information. Furthermore, there should be, where practical, separation of duties between authorised users assigned to the development/test environment(s) and to those assigned to the production environment.

Contact with authorities

(17) The University aims for compliance with the NSW Cyber Security Policy as maintained by the NSW Department of Finance Services and Innovation.

(18) The University aims for compliance with the Notifiable Data Breaches scheme as maintained by the Office of the Australian Information Commissioner. Refer to the University Information Technology Procedure - Personal Data Breach.

(19) The University will comply with all registration, reporting and operational requirements of the Security of Critical Infrastructure Act 2018.

Contact with special interest groups (SIGs)

(20) The Division of Information Technology ICT Security Team should maintain appropriate contacts with special interest groups or other specialist security forums and professional associations including:

a. AusCERT (Australian Cyber Emergency Response Team)
b. Council of Australasian University Directors of Information and Technology (CAUDIT)
c. Australia's Academic and Research Network (AARNet)
d. Australian Cyber Security Centre (ACSC)

Information security in project management

(21) Information security must be integrated into the University's project management methods to ensure that information security risks are identified and addressed throughout all stages of a project. Refer to the DIT Project Security Considerations Guide.

Part B - Human resource security

Objective

(22) To ensure that all authorised users:

a. understand their information and communication technology (ICT) responsibilities
b. are suitable for the roles they are considered for
c. do not engage in theft, fraud, and/or misuse of ICT facilities.

Prior to employment

(23) All authorised users should understand their responsibilities towards handling the University's information. Information security responsibilities should be addressed prior to, or on commencement of, employment through adequate job descriptions and in the terms and conditions of employment.

Screening

(24) Background verification checks should be carried out on all candidates for employment, including contractors, volunteers and third-party users. The checks should be proportional to business requirements, the classification of the information to be accessed, and the perceived risks. Applications for employment involving access to the University's facilities require a background screening process that is commensurate with the sensitivity of the information to be accessed during employment, and the system privileges required for the job function.

(25) Screeing for potential and current employees will be in accordance with the Employment Screening Procedure

(26) Screening procedures should also be carried out for agents, contractors, volunteers, and third-party users where appropriate.

(27) Where contractors are provided through a recruitment agency, the contract with the recruitment agency should clearly specify the agency’s responsibilities for candidate screening, notwithstanding the notification procedures to be followed if screening has not been completed, or if results give cause for doubt or concern. In the same way, the agreement with the third party should clearly specify all responsibilities and notification procedures for screening.

Terms and conditions of employment

(28) As part of contractual obligations, authorised users must sign the terms and conditions of their employment contract.

(29) Contractors, volunteers, and other authorised third-party users must sign a contractual agreement or an equivalent privacy and security agreement. The agreement should state the individual and University responsibilities for information security. See also the Finance Procedure - Contractors and Consultants.

(30) The terms and conditions of employment or engagement should reflect the requirement to comply with all University policies and procedures.

(31) Individuals that are not engaged via a University employment process (e.g. engaged via a third-party organisation) are to be treated to the same information security procedures as defined for employees. This must be followed prior to the granting of access to the University's ICT systems.

(32) Confidentiality agreements with the individuals may only be omitted if an existing contract with the third-party specifies appropriate confidentiality requirements.

During employment

(33) Authorised users must be aware of:

a. information security threats and concerns
b. their responsibilities and liabilities defined in employment or contractual agreements.

(34) Management responsibilities should also be defined in position descriptions to ensure information security is applied throughout an individual's employment within the University.

(35) An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to all authorised users to minimise possible information security risks.

Management responsibilities

(36) Management should require authorised users apply information security in accordance with established University policies, standards, and procedures. Management responsibilities should include ensuring that authorised users:

a. are adequately briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems
b. are provided with guidelines that state information security expectations of their role within the University
c. achieve a level of awareness on information security relevant to their roles and responsibilities within the University
d. conform to the terms and conditions of their employment
e. are issued with a new access card or badge that has the appropriate access rights.

(37) Access rights should be reviewed by system custodians on a regular basis to ensure that permissions are reflective of the activities being carried out by the individual. It is also recommended that ICT security responsibilities be added to job descriptions for management position responsibilities where relevant.

(38) Training should be provided to managers with ICT security responsibilities where required.

Information security awareness, education and training

(39) A formal information security awareness program should be implemented to provide all authorised users awareness around the importance of information security, cardholder data security and privacy. The program should educate users on information security problems and incidents and how they could respond to problems and incidents according to the needs of their work role.

(40) The University's security awareness program should include multiple methods of communication (e.g. posters, emails, memos, web-based training, meetings and promotions) to educate authorised users. All authorised users should receive appropriate information security awareness training and regular updates as relevant for their job function.

(41) Information security awareness training must be conducted during employee induction and annually thereafter as referenced in the Information Technology Procedure - Acceptable Use and Access. This training should be incorporated into standard employee orientation and education processes.

(42) Information security awareness, education and training activities should:

a. be suitable and relevant to the authorised user's roles, responsibilities, and skills
b. include information on known threats
c. provide contact details for further information and security advice
d. list the proper channels for reporting information security incidents.

(43) Authorised users should receive training in the correct use of ICT facilities and information on disciplinary processes, prior to the granting of access to ICT services. Refer to the Information Technology Access and Induction Procedure for further information.

Termination and change of employment

(44) All authorised users departing the University or changing roles should be governed by termination and change of employment processes conducted in an orderly manner. Changes to roles and responsibilities within the University should also be managed, notwithstanding, management of the termination of the respective responsibility or employment in line with this document.

(45) Responsibilities should be in place to ensure that the authorised user's exit from the University is managed and that the return of all equipment, information assets and removal of all access rights is completed. The departing authorised user should be reminded of continuing nondisclosure obligations after leaving.

Termination or change of employment responsibilities

(46) The University's Division of People and Culture (DPC) is generally responsible for the overall termination process, working together with the supervising manager of the authorised user leaving to manage the information security aspects of the relevant procedures.

(47) Supervisors must co-ordinate exits and changes with DPC to ensure appropriate computer systems and building access is maintained or revoked.

(48) In the case of a contractor, this termination responsibility process may be undertaken by the agency responsible for the contractor, and in the case of other users (e.g. service providers), this might be handled by their respective organisation.

(49) The communication of exit responsibilities should include:

a. ongoing information security requirements and legal responsibilities
b. responsibilities contained within any confidentiality agreement and continuing these for a defined period after the end of the employee's, contractor's, and/or third-party user's assignment.

(50) Changes of responsibility or employment should be managed as the termination of the respective responsibility or employment, and the new responsibility or employment should be controlled.

Part C - Asset management

Objective

(51) To ensure integrity of the University's information assets and that data confidentiality is maintained when equipment or services are established, replaced, decommissioned or serviced. This section also includes the handling, control and disposal of storage media.

Responsibility for assets

Inventory of assets

(52) Business critical assets should be identified and maintained in the appropriate asset register – Applications Portfolio, Data Assets Register or Infrastructure Assets Register.

Custodianship of assets

(53) Asset custodians must be assigned to all assets identified and be recorded within the respective asset register. Asset custodians should work with the Division of Information Technology to determine appropriate classification levels for their information assets and make decisions about authorised users permitted to access and use the information.

(54) The responsibility of an asset custodian is to:

a. work with the Division of Information Technology to ensure appropriate risk management process are implemented
b. maintain the currency of asset registers to define and maintain specific security control procedures (e.g. access control)
c. implement and maintenance of measures for control effectiveness
d. provide recovery capabilities consistent with the requirements of the University.

Acceptable use of assets

(55) The Information Technology Procedure - Acceptable Use and Access defines:

a. appropriate use of computing and communications resources
b. information stored on or transmitted via the University's computers, networks, telephones and/or other communications devices.

Return of assets

(56) All authorised users must return all University assets in their possession upon termination of their employment, contract or agreement. The termination process should be formalised in accordance with Part B and should include the return of all previously issued software, corporate documents and ICT equipment. This includes:

a. mobile computing devices
b. keys
c. access cards
d. software
e. manuals
f. all University-owned information stored on electronic media.

(57) In cases where an authorised user has university operational knowledge, that information should be documented and transferred to the University. Where the authorised user plays a role in information security plans (e.g. incident response procedure or contingency plan), respective plans must be updated accordingly.

Removal and secure disposal or reuse of equipment

(58) Sensitive information must be removed from any information system equipment that has been used for University business prior to its disposal, donation or re-use.

(59) Disposal of equipment should be undertaken as per the Information Technology Procedure – Purchasing and Disposal.

Information classification

Classification of information

(60) Classifications and associated protective controls for information and/or information assets must be in accordance to the business requirements of sharing and/or the restriction of information, inclusive of, the business impacts associated with such requirements. Classification guidelines have been developed, implemented and communicated to all University information asset custodians. Information and/or information assets must be classified in terms of value, legal requirements, sensitivity and criticality to the University.

(61) The University Information Classification and Handling Procedure requires information assets to be protectively marked into one of four classifications. The way the data is handled, published, moved and stored will be dependent on this scheme.

Handling of information assets

(62) Internal procedures exist for the handling, processing, storing and communicating of information and/or information assets in accordance with the Information Classification and Handling Procedure adopted by the University. Refer to the Data Access Form.

Media handling

Management of removable media

(63) The management of computer media must be controlled.

(64) Individuals must take appropriate steps to ensure the security of any computer media removed from the University. All media, in accordance with the classification of the data stored on the media, must be stored in a safe and secure environment.

(65) Remote users who may or may not have direct access to the University network must ensure that data, which is backed up to removable media, uses strong encryption methods and is stored in a secure manner.

(66) Classification of such data should be determined in collaboration with data and/or business custodian and the Enterprise Architect, Information.

Disposal of media

(67) All computer media must be disposed of securely and safely when no longer required. Refer to the Information Technology Procedure - Purchasing and Disposal.

(68) Disposal of University information must be in accordance with the Records Management Policy and Records Management Procedure.

(69) Physical media containing data that is no longer required must be either:

a. physically destroyed using the secure University disposal service
b. degaussed (decreasing or eliminating a remnant magnetic field)
c. rendered irretrievable using secure sanitisation software.

(70) For hard-copy materials, acceptable methods of disposal include:

a. shredding
b. incineration
c. pulping.

Part D - Access control

Objective

(71) To detail access control requirements for information and/or information processing facilities.

Business requirements of access control

Access Control

(72) Business requirements for access control must be defined and documented with access to system components and/or sensitive information restricted to only those individuals whose job requires such access. All authorised users with provisioned access should be given a clear statement of the business requirements which must be met by the access controls.

(73) All authorised users must have a single unique user ID and a password for access to any aspect of the University's ICT systems.

(74) Shared, generic or group user IDs and/or passwords must not be created nor used. Conference accounts must be restricted to internet access only.

(75) Access to privileged accounts must be restricted to the least privilege level necessary to perform job responsibilities.

(76) Assignment of privileges must always be based on each individual's job classification and function as per the Delegations and Authorisations Policy. Levels of privileges required for each role (e.g. user, administrator) for accessing resources must be defined.

(77) Documented approval by system custodians is required for all access, specifying required privileges. Access controls should be implemented via automated access control systems (e.g. Identity and Access Management systems) with access control roles (e.g. access request, access authorisation, access administration) implemented with appropriate separation of duties.

User access provisioning

(78) Each user must be allocated access rights and permissions to computer systems and data that correspond with the tasks they are expected to perform in accordance with the Information Technology Procedure - Acceptable Use and Access. This should be role-based (e.g. a user account will be added to a group that has been created with access permissions required by that job role).

(79) A request for temporary access via the Temporary Access Administration System to the University's network and/or computer systems must include a declaration by the account supervisor that appropriate checks have been carried out and correct authorisation obtained prior to temporary access account creation.

User access de-registration

(80) When an employee departs the University under normal circumstances, the termination of access shall be performed in accordance with the standard process as triggered by the human resources management system and implemented by the Identity and Group Management System (IGMS).

(81) For services not managed by IGMS, it is the responsibility of the systems custodian to ensure suspension of access for authorised users that have ceased employment with the University.

(82) In exceptional circumstances where there is perceived to be a risk that such employee may take action that will harm the University prior to or upon termination, a request to remove access may be approved and actioned by senior management (including Directors, Executive Directors, Deans and Heads of School) in advance of notice of termination being given. This precaution should especially apply in the case where the individual concerned has privileged access rights (e.g. domain administrator rights).

(83) User accounts should be initially suspended or disabled only and not deleted. User account names should not be

reused as this may cause confusion in the event of a later investigation.

Remote work

(84) The University must provide secure remote access services to enable authorised users to work from a remote worksite. Appropriate controls must be implemented to authorise and control remote work activities.

(85) Any remote access for work purposes should employ multifactor authentication mechanisms (e.g. 2-Step Verification, SMS codes) where provided.

(86) Authorised users must structure their remote working environment so that it is compliant with the Employment Conditions Procedure - Workplace Attendance.

(87) When using direct remote access services (e.g. virtual private network – VPN), authorised users should use managed University devices that are kept up to date with current operating system and application software updates, and a current anti-virus solution.

(88) Remote access using personal computing devices should use gateway services (e.g. virtual desktop infrastructure – VDI).

(89) Direct remote access using personal computing devices must be approved by the Manager, Infrastructure and provisioned via the IT Service Desk.

(90) Remote access service usage will be logged and recorded, including user name and logon/off times.

Vendor remote access

(91) Vendor access to the University's computer systems is granted solely for the work commissioned and for no other purposes.

(92) Vendors must comply with all applicable University policies, standards and agreements.

(93) Vendor agreements and contracts should specify:

a. agreed methods and technologies required to facilitate remote access
b. University information and systems the vendor should have access to. If, at the time of contract negations this is unknown or ambiguous, mention of this should be made in the agreement
c. how University information is to be protected by the vendor. A copy of the vendor’s security and privacy policy should be made available to the University where appropriate
d. acceptable methods for the return, destruction or disposal of University information in the vendor’s possession at the end of the contract
e. agreement that the Vendor must only use University information and information systems for the purpose of the business agreement
f. any other University information acquired by the vendor in the course of the contract cannot be used for the vendor’s own purposes or divulged to others.

(94) Approval for vendor remote access should be sought via the system custodian or relevant manager.

(95) Privileged level access will be monitored and logged as per ‘Management of privileged access rights’ below.

(96) Before accessing University information systems and, unless covered by an existing contract or agreement, an authorised representative of the vendor must sign the Division of Information Technology Vendor Security, Privacy, Copyright and Confidentiality Agreement Form.

(97) For vendors using a generic University account for remote access, contracts or agreements must include a requirement to inform the University of vendor staff moves and changes. Passwords must be changed as per the Information Technology Procedure - Passwords.

Review of user access rights

(98) On a regular basis (at least twice a year), asset and system custodians will be required to review and document who has access to their areas of responsibility and the level of access in place. This identifies:

a. people who should not have access (e.g. those who have left the University)
b. user accounts with more access than required by the role
c. user accounts with incorrect role allocations
d. accounts with extended periods of inactivity
e. accounts belonging to authorised users on long periods of leave
f. generic accounts
g. user accounts that do not provide adequate identification (e.g. generic or shared accounts)
h. accounts that breach segregation of duties
i. any other issues.

System and application access control

(99) As part of the evaluation process for new or significantly changed systems, requirements for effective access control should be addressed and appropriate measures implemented.

(100) These should consist of a comprehensive security model that includes support for, but not limited to:

a. creation of individual user accounts
b. definition of roles or groups which user accounts can be assigned
c. allocation of permissions to objects (e.g. files, programs, menus) of distinct types (e.g. read, write, delete, execute) to subjects (e.g. user accounts and groups)
d. provision of varying views of menu options and data according to the user account and its permission levels;
e. user account administration (e.g. ability to disable and delete accounts)
f. user logon controls:
    i. non-display of password as it is entered
    ii. account lockout once number of incorrect logon attempts exceeds a specified threshold
    iii. information about number of unsuccessful logon attempts and last successful logon once user has successfully logged on
    iv. date and time-based logon restrictions
g. device and location logon restrictions
h. user inactivity timeout
i. password management:
    i. ability for user to change password
    ii. controls over acceptable passwords
    iii. password expiry
j. hashed/encrypted password storage and transmission
k. security auditing facilities
    i. logon/logoffs
    ii. unsuccessful logon attempts

iii. object access
iv. account administration activities.

Access control considerations for new services

(101) As part of the selection of cloud service providers specifically, the following access-related considerations must be observed:

a. user registration and deregistration functions provided
b. facilities for managing access rights to the cloud service
c. extent access to cloud services, cloud service functions and cloud service customer data can be controlled on an as required basis
d. availability of multi-factor authentication for administrator accounts
e. procedures for the allocation of secret information (e.g. passwords).

(102) Addressing these requirements as part of the selection process will ensure that the provisions of this document can be met in the cloud, as well as within on-premise systems.

Management of privileged access rights

(103) Privileged access rights such as those associated with administrator-level accounts must be identified for each system or network and tightly controlled. In general ICT support staff and other technical users should not make day to day use of user accounts with privileged access, but rather a separate “admin” user account should be created and used only when additional privileges are required. These accounts should be specific to an individual (e.g. “John Smith Admin”). Generic admin accounts must not be used as they provide insufficient identification of the user.

(104) Access to admin level permissions should only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.

(105) User accounts must not be used for privileged access in automated routines such as batch or interface jobs or as service accounts.

(106) Approval for the granting of privileged access rights, and the authorisation level of those rights is at the discretion of the identified system or application custodian.

(107) Day to day management of privileged access rights are the responsibility of the delegated system or application administrator.

(108) The activity of privileged accounts should be monitored and logged including but not limited to:

a. logon/logoff times
b. commands issued
c. information accessed, copied or moved.

(109) Logs should be protected from unauthorised access and modification.

Use of secret authentication information

(110) Users are bound by the Information Technology Procedure - Passwords. Quality and complex passwords must be enforced, with the quality and complexity of passwords created by users enforced by controls in the password management system.

System and application access control

Information access restriction

(111) Access to information and application system functions must be restricted in accordance with the University Information Technology Procedure - Acceptable Use and Access. All information stored on a computer that is sensitive, critical, and/or valuable, must have system access controls to ensure that they are not improperly disclosed, modified, deleted, or rendered unavailable.

(112) User privileges must be defined so ordinary users cannot gain access to, or otherwise interfere with, either the individual activities or private data of other users.

Secure logon

(113) Access to operating systems must use a secure logon process, with physical access to business information system hardware restricted.

(114) If any part of a logon sequence during the logging into a computer or data communications system process is incorrect, the user must only be given feedback that the entire logon process was incorrect.

(115) Every logon screen for multi-user computers must include a special banner stating that:

a. the system may only be accessed by authorised users
b. only authorised users may logon
c. system usage will be monitored and logged
d. unauthorised system usage or abuse is subject to criminal prosecution.

Password management system

(116) A formal password management system must be enforced. This password management system must include various password controls such as, but not limited to:

a. compliance with the Information Technology Procedure - Passwords
b. the recording of individual's password management actions
c. the enforcement of regular password changes
d. the storage of passwords in an unrecoverable format.

(117) Information systems must not use vendor supplied defaults for system passwords and other security passwords.

(118) Users are bound by the University Information Technology Procedure - Passwords requiring users to follow industry best security practices in the selection and usage of passwords.

Use of privileged utility programs

(119) All information system tools and utilities that may be used to either cause significant damage and/or override systems must automatically be restricted to authorised users for intended usage purposes.

Access control to program source code

(120) Access to program source code must be restricted to authorised employees and agents and on a need-to-know basis only.

Mobile devices

(121) Only managed personal computing devices are to be given privileged network access to critical University information systems.

(122) Non-managed mobile devices are not given privileged network access unless exemption has been granted by the Chief Information and Digital Officer or nominee.

(123) Policies and supporting security measures should be adopted to manage the risks introduced by using managed devices. Appropriate controls must also be implemented to protect against the risks of working with mobile computing facilities used in unprotected environments.

(124) All managed and non-managed mobile devices containing sensitive information must employ storage encryption for all files.

(125) The University provides selected authorised users with portable computer equipment so that they may perform their jobs at remote locations. Information stored in University portable computer equipment is University property and may be inspected or analysed in any manner at any time by the University.

(126) Similar to University owned equipment, such equipment must be returned to the University on cessation of employment with the University.

(127) All authorised users must keep all portable devices containing University information in their possession, unless stored and/or deposited in a secure location.

Part E - Cryptography

Cryptographic controls

Objective

(128) To ensure proper and effective use of cryptography to protect the confidentiality of information in the event of unauthorised access or interception.

Use of cryptographic controls

(129) Data classified as highly confidential and/or confidential/private should be encrypted in transport over the internet as well as in storage. However deciding as to whether a cryptographic solution is appropriate must be part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine:

a. whether a cryptographic control is appropriate
b. what type of control must be applied
c. what purpose and operational process applies to such control.

(130) Specialist advice should be sought from the Division of Information Technology ICT Security Team. This is to:

a. identify the appropriate level of protection
b. define suitable specifications that will provide the required protection and support for the implementation of a secure key management system.

Key management

(131) If encryption technology is in use, key management must be in place to support the University's usage of cryptographic techniques. Key management policies and procedures must address that all cryptographic keys be

protected against:

a. modification
b. loss
c. destruction
d. unauthorised disclosure (secret and/or private keys)
e. equipment used to generate, store and archive keys (which must be physically protected).

(132) Key management policies and procedures specified to protect keys used for the encryption of sensitive and/or critical data against disclosure and misuse, should include, but not be limited to:

a. the restriction of the fewest number of custodians necessary for access to keys
b. key-encrypting keys are at least as strong as the data-encrypting keys they protect
c. key-encrypting keys are stored separately from data-encrypting keys
d. keys are stored securely in the fewest possible locations and forms
e. the crypto period(s) for each key type in use is defined, inclusive of the process for key changes at the end of the crypto period(s)
f. the retirement or replacement of keys when the integrity of the key has been weakened
g. the replacement of known or suspected compromised keys
h. any keys retained after the retirement or replacement of such keys are not used for encryption operations
i. a process specifying how to generate strong keys, how to securely distribute keys and how to securely store keys
j. a process preventing the unauthorised substitution of keys
k. a process for key custodians to acknowledge (in writing or electronically) their understanding and acceptance of key-custodian responsibilities.

Part F - Physical and environmental security

Objective

(133) To detail the physical security requirements for the University such as computer room requirements, guarding, physical locks, and the security structure of all relevant premises within the offices of the University.

Secure areas

Physical security perimeter

(134) The University must define and use an appropriate security perimeter to protect areas such as data centres, which contain information processing facilities. Perimeter security barriers such as walls, card controlled entry gates and/or manned reception desks, should be utilised dependent on the level of physical security required.

(135) Data centre physical security must be reviewed at least annually.

Physical entry controls

(136) Remote data centre physical entry controls are governed by the data centre operator contracted to the University to provide data centre services.

(137) On-campus physical entry controls are governed by the Facilities and Premises Procedure - Access, Use and Security.

(138) Secure areas must be protected by appropriate entry controls to ensure that only authorised users are allowed access. CCTV cameras and/or other access control mechanisms must be used to monitor individual physical access to sensitive areas. Such mechanisms must be protected from tampering and/or disabling.

(139) Access logs must be stored for at least three months, unless otherwise either restricted by law or increased by a subsequent standard or guideline.

(140) Access to office, computer room, or work areas containing sensitive and/or critical information must be physically restricted, with access only provided to those with a valid business need. Authorised user access lists must be periodically reviewed with access revoked for individuals no longer requiring access.

(141) Documented processes and/or procedures for assigning identification cards (e.g. badges) to onsite authorised users and visitors must exist. Such processes and/or procedures must define:

a. the granting of new identification cards
b. the changing of access requirements
c. the revocation of identification cards for terminated onsite authorised users.

(142) Authorised users who can access the identification card generation and/or access control system(s) must be documented and periodically reviewed.

(143) Visitor logs for data centre and secure areas must be retained for at least three months and contain the:

a. visitor’s name
b. organisation represented
c. onsite physical access.

(144) All authorised users must wear an identification badge on their outer clothing when in data centres and/or facilities that store sensitive and/or critical University data. This identification must be clearly visible and distinguishable between onsite authorised users and visitors.

(145) Employees must not permit unknown or unauthorised users access through doors, gates, and/or other entrances to restricted and/or sensitive areas.

Securing sensitive offices, rooms and facilities

(146) Controlled areas should be created to protect offices, rooms, and facilities that should not be open to general or public access. All employees must ensure doors to sensitive areas, rooms, and/or information processing facilities are locked, preventing unauthorised access when not in use. Physical and/or logical controls must be implemented, restricting access to publicly accessible network connection points.

Protecting against external and environmental threats

(147) Information systems must be housed in a secure manner, protected from external and environmental threats to the premises. Such threats include, but are not limited to:

a. theft
b. tampering
c. damage
d. destruction
e. flood
f. fire.

(148) Data centres must have:

a. fire detection and suppression
b. power conditioning
c. air conditioning
d. humidity control
e. other computing environment protection
f. appropriate intrusion alarm systems automatically alerting authorised users to take immediate action.

Working in secure areas

(149) Additional controls and guidelines for working in sensitive areas must be used to enhance the security provided by the physical controls protecting the secure areas. Access to sensitive areas must be authorised and based on individual job functions with access revoked immediately upon termination.

Delivery and loading areas

(150) Delivery and loading areas should be controlled, and where possible, isolated from information processing facilities to avoid unauthorised access.

Information and communication technology (ICT) equipment

Equipment location and protection

(151) On-premise equipment must be located and/or protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorised access.

(152) Physical access to networking and/or communications hardware must be restricted by appropriate physical controls. All business critical production computer systems including, but not limited to servers, firewalls, proximity access control, systems, and/or voice mail systems must be physically located within a secure data centre.

(153) Authorised users should be encouraged to report detection of tampering and/or the substitution of devices. Training should include, but not be limited to:

a. how to verify the identity of any third-party persons claiming to be repair or maintenance staff, prior to granting them access to modify or troubleshoot devices
b. obtaining verification prior to installing, replacing, and/or returning devices
c. being aware of suspicious behaviour around devices (e.g. attempts by unknown persons to unplug or open devices)
d. encouragement to report suspicious behaviour and indications of device tampering or substitution to appropriate staff (e.g. manager or security officer).

Supporting utilities

(154) Key ICT equipment must be protected from power failures and surges and other electrical anomalies. Uninterruptible power supply (UPS) systems, line conditioners, electrical power filters, and/or surge suppressors must be used for business critical ICT infrastructure.

(155) Critical supporting utilities must be tested on a regular basis to ensure equipment has adequate capacity, in accordance with the manufacturer’s recommendations.

Cabling security

(156) Power and telecommunications cabling carrying data and/or supporting information services must be protected from interception or damage. Installation and maintenance of power and telecommunication cabling must follow current industry security standards.

Equipment maintenance

(157) Equipment sent off-site for maintenance purposes must have any sensitive or confidential information erased to ensure the confidentiality and integrity of information.

Unattended user equipment

(158) Users must ensure that unattended equipment contains appropriate protection and/or security controls when unattended. If the computer system to which an authorised user is connected contains sensitive information, the authorised user must not leave their personal computer, workstation, or terminal unattended without locking or logging out.

Clear desk

(159) Unless information is in active use by authorised users, desks must be clear and clean during non-working hours with sensitive information locked away.

Part G - Operations security

Operational procedures and responsibilities

Objective

(160) Operations security aims to:

a. secure the operation of information processing facilities
b. implement and maintain the appropriate level of information security on information assets
c. minimise the risk of system failures
d. protect and maintain the integrity and availability of information and information processing facilities
e. ensure the protection of information in networks and the protection of the supporting infrastructure
f. prevent unauthorised disclosure, modification, removal or destruction of assets and interruption of business activities
g. maintain the security of information exchanged within the University and with any external party
h. detect unauthorised information processing activities
i. protect information system against an individual falsely denying having performed an action.

Documented operating procedures

(161) Operating procedures for information systems must be documented and maintained. Operating procedures must include, but not be limited to:

a. procedures for processing and handling information
b. instructions for handling errors or other exceptional conditions
c. include support contacts for unexpected operational or technical difficulties.

Change management

(162) Nonstandard changes to information processing facilities and systems must be documented and controlled via the University Change Advisory Board (CAB). Extensions, modifications, and/or replacements to production software and hardware must be performed only when approval from CAB has been received prior to the proposed change window start time.

(163) A change control procedure for all changes is defined and includes the:

a. documentation of impact
b. documented approval by authorised parties
c. testing of functionality to ensure such change does not adversely impact the security of the system
d. testing of all custom code updates for compliance with industry standards and requirements where applicable
e. back-out, and/or change rollback procedures
f. communications plan ensuring relevant stakeholders are aware of any potential impact.

(164) Risk assessments and/or vulnerability assessments must be conducted when implementing new systems or making significant changes to existing systems.

(165) Adequate rollback procedures must be developed for all changes to production systems ensuring information processing in the case of a change failure can be promptly restored to the respective state prior to the most recent change.

(166) All changes to information processing facilities must be communicated to all relevant authorised users. Changes to the environment may also trigger the requirement to perform specific security tests, inclusive of, but not limited to vulnerability assessments and penetration tests confirming that changes made have not inadvertently degraded the security profile of the University.

Capacity management

(167) Capacity demands must be monitored with projections of future capacity requirements made to ensure that adequate processing power, storage and other required resources are available.

Separation of development, testing and operational environments

(168) Facilities and functions used in the development of computing solutions, notwithstanding their respective testing, must strictly be kept separate from production systems. This is to reduce the likelihood of accidental, and/or unauthorised changes to production systems, subsequently creating operational problems and/or compromising the University’s related information.

(169) Separation can be achieved through physical or logical separation, appropriate to the sensitivity of the information and/or functions of the system concerned.

Protection from malware

Control against malware

(170) Detection and prevention controls to protect against malware and appropriate user awareness procedures must be implemented. Approved anti-malware software must be deployed across the University network to all systems, remain enabled, and contain regular definition updates and scanning.

(171) Anti-malware solutions and/or other appropriate controls should also be implemented and configured to prevent or detect the use of:

a. unauthorised software on information systems (e.g. server application whitelisting)
b. known or suspected malicious websites (e.g. blacklisting), and generate software logs with such logs retained for at least one year.

(172) Anti-malware mechanisms must be confirmed as actively running and cannot be disabled or altered by users unless specifically authorised by management on a case-by-case basis for a limited period.

(173) Systems that are malware-infected must be disconnected from the network until such time when the anti-malware software has been updated and all malware eradicated.

(174) Appropriate content filtering mechanisms must be deployed to protect all user initiated connections. Formal measurement and reporting procedures must also be implemented to record the number and severity of actual or suspected malicious code incidents.

Backup

Information backup

(175) The University must ensure backup facilities are provided and used. Backup strategies are developed in collaboration with system custodians and contain copies of essential business information and software. All sensitive, valuable, and/or critical information recorded on backup computer media and stored outside University offices must be given an appropriate level of physical and environmental protection. Backup and restore procedures must be securely and adequately documented.

(176) Critical business information and critical software archived on computer storage media for prolonged periods must be tested at least annually providing assurance that such data can be completely and efficiently recovered.

(177) Refer to Appendix C for backup details.

Logging and monitoring

Event logging

(178) Audit logs must be produced for business critical systems, showing:

a. start and stop times for production applications
b. system boot and restart times
c. system configuration changes
d. system errors and corrective actions taken
e. confirmation of correct handling of files and related output.

(179) Audit trails must be retained for at least one year. Audit trails must be implemented to link all system component access to each individual user. For event reconstruction, audit trails should contain event information that may include, but not limited to:

a. privileged account system activities
b. individual user accesses to sensitive information
c. all changes to access controls at the network, operating system or application layers
d. access to all audit trails
e. invalid access attempts
f. use of and changes to identification and authentication mechanisms. This includes but is not limited to, the creation of new accounts, elevation of privileges and all changes, additions or deletions to accounts with root or

administrative privileges

g. initialisation, stopping, or pausing of the collection of audit logs
h. creation and deletion of system-level objects.

(180) Audit trail entries recorded for all system components for each event must contain, but not be limited to:

a. identification of the user involved
b. type of event
c. date and time of event
d. success and/or failure indication
e. origination or source of event
f. identity or name of affected data, system component or resource.

Protection of log information

(181) All system and application logs must be maintained in a form such that logs cannot be accessed by unauthorised users and are stored in a secure manner. Authorised users must have a readily demonstrable need for such access to perform their regular duties. All other authorised users seeking access to these logs must first obtain approval.

(182) Audit trails must be secured and promptly backed up to a centralised log server or to media that is difficult to alter. Only individuals with job-related needs may have access to view audit trail files.

(183) Log information should be exported to a security information and event monitoring solution for automated analysis, alerting and actioning.

Administrator and operator logs

(184) Activities of administrators and operational staff must be logged. These logs must be kept for at least one year with a minimum of three months available online and not be altered by anyone. These logs must be subject to regular and independent checks.

Clock synchronisation

(185) Time synchronisation technology such as the Network Time Protocol (NTP) must be used to synchronise all critical system clocks, dates, and times.

Control of operational software

Installation of software on operational systems

(186) Updating of operational program libraries must only be performed by nominated administrators or system custodians following appropriate authorisation. Configuration management processes should be used to keep track and control all implemented software as well as related system documentation. Changes to operational systems must undergo the formal change management processes.

Technical vulnerability management

Management of technical vulnerabilities

(187) Systems must be in place for the timely gathering of information about technical vulnerabilities of information systems. Processes must be established to identify new security vulnerabilities using reputable outside sources for security vulnerability information.

(188) The University's exposure to these vulnerabilities must be evaluated with appropriate measures taken to address the associated risk across the University.

(189) All patches and security updates should be pushed out in a formalised and secure manner with all critical or high-ranking patches installed within one month of vendor release or other approved third party. Installation of all remaining applicable vendor supplied security patches should be applied within an appropriate period (e.g. within three months).

(190) For internet accessible web applications, new threats and vulnerabilities must be addressed on an ongoing basis ensuring such applications are protected against known attacks. The installation of an automated technical solution that detects and prevents web-based attacks (e.g. a Web Application Firewall (WAF)) in front of public-facing web applications will allow continual checks of all traffic and generate alerts where applicable.

(191) A documented process to review the security of public-facing web applications using either manual or automated tools or methods must exist. These processes must be reviewed:

a. at least twice a year
b. after any changes
c. by an organisation that specialises in application security
d. once all vulnerabilities are corrected.

(192) Such web application must be re-evaluated post remediation actions.

Restrictions on software installation

(193) An authorised user shall not introduce software or technology designed to disrupt, corrupt or destroy programs and/or data, or sabotage University ICT facilities as per the Information Technology Procedure - Acceptable Use and Access.

(194) Access rights for the installation of software should follow the principle of least privilege.

Information systems audit considerations

Information systems audit controls

(195) Audits of operational systems must be planned and agreed upon to minimise the risk of disruptions to business processes. Audit requirements, scope and access other than read-only must be authorised by the University with adequate resources provided. Procedures, requirements and responsibilities must be documented with all access monitored and logged.

Part H - Communications security

Network security management

Objective

(196) To ensure the protection of information in networks and its supporting information processing facilities.

Network controls

(197) Controls must be implemented to achieve and maintain performance, reliability and security in networks inclusive of information in transit. Firewalls must be installed at each internet connection between any de-militarised zone (DMZ) and/or intranets and between any wireless network.

(198) Configuration standards must be documented, implemented, updated and referenced for the installation and administration of all firewalls and routers. Rule sets and/or access control lists (ACLs) of firewalls and/or routers must be reviewed at least every six months. Configuration standards must include a description of groups, roles, and responsibilities for management of network components. They must also include a list of all services, protocols and ports necessary for business, inclusive of business justifications for protocols considered to be insecure.

(199) All data transmitted over open public networks must be secured using strong cryptography and security protocols including, but not limited to TLS (transport layer security), and/or IPsec. A process should also be specified for:

a. the acceptance of only trusted keys and/or certificates
b. the protocol in use to only support secure versions and configurations (e.g. that insecure versions or configurations are not supported)
c. the implementation of proper encryption strength per the encryption methodology in use.

(200) Configurations and related parameters on all hosts attached to the University network must comply with current policies and standards. Security risk assessments must be conducted as a part of network design processes with such assessments carried out when introducing new network services or making significant changes to existing services.

(201) All administrative access must be encrypted using security protocols, including but not limited to SSH (Secure Shell), VPN, or TLS. This applies to both web-based management and other administrative access. Responsibilities and procedures for the management of the network must also be established and documented.

(202) Network diagrams and configurations including connections to other systems and networks must be maintained and kept current. Network diagrams must identify all connections between the environments containing critical and/or sensitive data and other networks including any wireless networks.

(203) For critical business systems, methods to obscure IP addressing must be in place to prevent the disclosure of the private IP addresses and routing information from internal networks to the Internet. Such methods may include, but are not limited to:

a. Network address translation (NAT)
b. placing servers containing critical and/or sensitive data behind proxy servers and/or network load balancers
c. removal or filtering of route advertisements for private networks that employ registered addressing
d. internal usage of RFC1918 private address space instead of public addresses.

(204) Personal firewall software must be installed and active on any managed or non-managed devices used to access University’s network infrastructure that also connects to the Internet when outside of the University network. Personal security software must not be alterable by users of managed or non-managed devices. Security policies and operational procedures for managing firewalls should be documented, in use, and known to all affected parties.

Security of network services

(205) Clear descriptions of security attributes, service levels and management requirements for all network services used by the University must be provided, inclusive of service level agreements and monitoring for services provided in-house or outsourced.

Segregation in networks

(206) Controls must be implemented in networks to segregate groups of information services, users and information systems. Security risk assessments must be conducted as a part of network design processes with such assessments carried out regularly on data networks.

Information transfer

Information transfer policies and procedures

(207) When transferring confidential or private information outside of the University, procedures and controls must be developed and implemented to protect the exchange, confidentiality and integrity of information.

Agreements on information transfer

(208) Formal agreements must be established for the electronic and/or manual exchange of information between the University and other organisations, third parties or clients.

Electronic messaging

(209) All employees of the University with access to email facilities are bound by the Information Technology Procedure - Acceptable Use and Access.

Confidentiality or non-disclosure agreements

(210) Where no contractual agreement exists, confidentiality and/or non-disclosure agreements reflecting the needs of the University for the protection of information should be used, regularly reviewed and documented.

Part I - System acquisition, development, and maintenance

Objective

(211) To detail the specific criteria around the acquisition, development and maintenance of information systems.

Security requirements of information systems

Information security requirements analysis and specification

(212) University system custodians and project managers must take security into consideration during all stages of system application development for both in-house and outsourced software development. The Division of Information Technology must be consulted on security requirements and specifications in the initial stages of project development. All software development efforts are to follow the defined processes for system and/or software development life cycle (SDLC), where security measures are defined at every stage of the entire process.

(213) Statements of business requirements for new information systems or enhancements to existing information systems must specify the requirements for information security controls. Risk assessment and risk management must be the base framework for analysing information security requirements and control identification. Security requirements and controls should reflect the business value of information assets involved and the potential business impact or loss, which may result from a failure or absence of security.

Securing application services on public networks

(214) Information involved in application services traversing public networks should be protected using strong encryption methods from fraudulent activity and unauthorised disclosure and modification.

Protecting application services transactions

(215) Information involved in application integration services should be protected to prevent:

a. incomplete transmission
b. misrouting

c. unauthorised message alteration
d. unauthorised disclosure
e. unauthorised message duplication and/or replay.

Security in development and support processes

(216) Rules for the development of software and systems should be established and applied to all developments within the University.

System change control procedures

(217) The implementation of changes must be controlled using the University Information Technology Infrastructure Library (ITIL) change management procedures. The change management procedures must also be used for the testing and implementation of security patches and software modifications.

Technical review of applications after operating platform changes

(218) When hosting environments and/or operating systems are significantly changed, business critical applications must be reviewed and tested to ensure there are no adverse impacts or information security risks to the application.

Restrictions on changes to software packages

(219) Modifications to vendor supplied software packages must be discouraged and/or limited to necessary changes. All changes must be strictly controlled, documented and approved via change control procedures.

Secure system engineering principles

(220) Guidelines for engineering of secure systems should be documented, maintained, reviewed and applied to any information system implementation efforts.

Virtualisation

(221) Virtualisation of systems can deliver increased operational efficiency in terms of hardware, network, storage and utilities usage. The security requirements of all virtualisation components must be considered.

(222) Most security vulnerabilities and threats apply equally to virtualised and physical environments however virtualisation may introduce additional security implications.

(223) All elements of a virtualisation solution must be secured and security maintained through software updates, configuration reviews and security testing.

(224) Administrator access to the hypervisor must be restricted, managed and monitored.

(225) Hypervisors and guest operating systems should be monitored for indicators of compromise.

Secure development environment

(226) The University should establish and appropriately protect secure development environments for system development and integration efforts, encompassing the entire system development lifecycle.

(227) Privileged access to development and test environments should use different credentials from those used to access production environments.

Outsourced development

(228) When outsourcing software development projects the University should consider:

a. licensing arrangements, code ownership, and intellectual property rights
b. certification of the quality and accuracy of the work carried out
c. escrow arrangements in the event of failure of the third party
d. rights of access for audit of the quality and accuracy of work done
e. contractual requirements for quality and security functionality of code
f. testing before installation (e.g. penetration testing, vulnerability testing, source code analysis) to detect malicious and/or Trojan code.

System security testing

(229) Testing of application security functionality should be integrated into development processes.

System acceptance testing

(230) Acceptance criteria for new information systems, upgrades and new versions must be established with suitable tests of the system carried out prior to acceptance. Requirements and criteria for acceptance of new systems must be clearly defined, agreed, documented and tested.

Test data

(231) Test data should be selected carefully and protected. Data masking or obfuscation should be used if using production data in development or test environments.

Protection of test data

(232) Test data, applications and related systems must be protected from unauthorised access and modifications. The use of operational databases containing sensitive and/or critical production data/information for testing purposes must be avoided.

(233) Confidential information such as Personally Identifiable Information (PII) used for testing purposes, inclusive of all sensitive details and content, should be protected for removal and/or modification. Production data must not be used for testing or development.

Part J - Supplier and cloud service provider relationships

Information security in supplier and cloud service provider relationships

Objective

(234) To ensure protection of the University's assets accessible by suppliers.

Information security procedures for supplier relationships

(235) Information security requirements for mitigating the risks associated with supplier access to University assets should be agreed with the supplier and documented.

(236) Any authorised users contemplating the use of cloud-based services, or the transfer or storage of University information externally, will first engage the services of the Division of Information Technology to ensure that resulting solution is viable and secure.

(237) The procurement of cloud services should be undertaken in accordance with the NSW Government Cloud Policy and the Division of Information Technology Project Security Considerations.

Addressing security within agreements

(238) All relevant information security requirements should be established and agreed upon with each supplier that may access, process, store, communicate, and/or provide ICT infrastructure components for the information of the University.

(239) Contractual agreements should consider and include the security considerations as described in the NSW Government Cloud Policy and the Division of Information Technology Project Security Considerations.

Supplier service delivery management

Monitoring and review of supplier services

(240) An established process for engaging service providers including proper due diligence prior to engagement should exist. The University must maintain a list of service providers along with a written agreement that includes an acknowledgement by the service provider of their responsibility for securing critical and/or sensitive data that the service provider possesses, or otherwise stores, processes, or transmits on behalf of the University.

(241) A formal review of service provider contracts and the compliance status of their security standards should be conducted when significant change occurs or on a regular basis as determined necessary for each provider. The frequency and depth of the review is based on level of risk, the services provided and classification of the information handled by the third party ensuring secure management practices are in place.

(242) Service providers should provide regular reports on the status of the services delivered to the University.

(243) The University should review reports regularly to ensure adherence to agreements.

(244) When required, service providers should allow the University, or an entity on its behalf, to audit the service provider's facilities, networks, computer systems and procedures for compliance in accordance with the agreed information security policies and standards.

Managing changes to supplier services

(245) Changes to the services provided by third parties are required to be managed. These include but are not limited to:

a. enhancements to the services provided
b. use of new technologies
c. adoption of new products, versions or releases
d. changes to physical location of service facilities.

(246) The management of changes should be in line with formal change control procedures. This includes consideration of business system criticality and processes involved for the re-assessment of risks.

Part K - Information security incident management

Objective

(247) To detail clear definitions of the types of incidents that are likely to be encountered and document a plan for corrective action.

Management of information security incidents and improvements

Responsibilities and procedures

(248) A consistent and effective approach should be applied to the management of information security incidents. Incident management responsibilities and procedures must be established to ensure quick, effective and orderly responses to security incidents and software malfunctions.

(249) Individuals responsible for handling information security incidents must provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies such as virus outbreaks and intrusions.

(250) Individuals responsible for handling information systems security incidents must have clearly defined responsibilities and be provided the authority to handle incidents and create security incident reports.

(251) The Division of Information Technology (DIT) is responsible for defining and operating a critical incident response process.

Reporting information security events

(252) Information security events associated with information systems must be reported to the IT Service Desk.

(253) A formal reporting and incident response procedure must be established for all breaches of information security, actual or suspected.

(254) All authorised users must be made aware of the procedure for reporting security incidents and the need to report incidents immediately.

(255) The DIT's critical incident response process must be tested at least annually and testing procedures must be in place.

Reporting information security weaknesses

(256) Any observed or suspected security weaknesses in, or threats to, systems or services must be reported to the IT Service Desk. All authorised users must be made aware of this and be instructed not to attempt to deliberately exploit suspected vulnerabilities.

Assessment of and decision on information security events

(257) Information security events should be assessed to determine whether they are to be classified as information security incidents.

Response to information security incidents

(258) Information security incidents should be responded to by the DIT ICT Security Team including other relevant authorised users of the University and/or external parties.

Learning from information security incidents

(259) Mechanisms must be in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored. An annual analysis of reported information security problems and violations must be prepared. Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Collection of evidence

(260) Where action against an individual or organisation involves the law, either civil or criminal, the evidence presented must conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in

which the case will be heard. This must include compliance with any published current standard and/or code of practice to produce admissible evidence.

Part L - Information security aspects of business continuity management

Information systems continuity

(261) Information systems continuity should be embedded within the University's business continuity management systems.

Planning information systems continuity

(262) A managed process regarding information systems availability requirements must be in place for the development and maintenance of business continuity throughout the University. Plans based on appropriate risk assessments must be developed as part of the overall approach to the University’s business continuity. This is described in the Information Technology Policy. The ICT Security Team in conjunction with the Division of Information Technology leadership oversee the implementation of this. The extent of such plans is dependent on the delivery of a business impact analysis (BIA).

(263) Such BIA must result in the specification of the:

a. maximum period that the University can go without critical information processing services
b. period in which management must decide whether to move to an alternative processing site
c. minimum acceptable production information system recovery configuration after a disaster or crisis.

Implementing information security continuity

(264) Plans must be developed to maintain or restore business operations in a timely manner following a disaster or crisis.

(265) The Information Technology Service Continuity Management (ITSCM) team must prepare and update a crisis management plan, covering topics such as:

a. a process for managing the crisis
b. crisis decision making
c. the safety of employees
d. damage control
e. communications with third parties such as the media.

(266) The ITSCM team will develop, implement and test business continuity and/or disaster recovery plans. Such plans must specify how alternative facilities such as, but not limited to telephones, systems, and networks, will be provided for authorised users to continue operations in the event of an interruption to, or failure of, critical business processes.

(267) All business continuity plans must consider the information security requirements of the University.

Verify, review and evaluate information security continuity

(268) The University should verify established and implemented information security continuity controls at reoccurring intervals ensuring such controls are valid and effective during adverse situations. Business continuity plans must be tested regularly by respective teams as outlined in the ITSCM and undergo regular reviews ensuring such plans are up to date and effective.

Redundancies

(269) Appropriate redundancy, as determined by required service levels, must be in place for critical systems and assets ensuring the availability of information processing facilities.

Availability of information processing facilities

(270) The University should identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using existing system architecture, redundant components and/or architectures should be considered.

(271) Where applicable, redundant information systems should be tested ensuring successful failover between components and/or other functions as intended.

Part M - Compliance

Objective

(272) To avoid breaches of legal, statutory, regulatory, and/or contractual obligations related to information security and/or other security requirements.

Compliance with legal and contractual requirements

Identification of applicable legislation and contractual requirements

(273) For every University production information system, all relevant statutory, regulatory and contractual requirements must be identified. This includes but is not limited to:

a. NSW Cyber Security Policy
b. NSW Government Cloud Policy
c. Privacy and Personal Information Protection Act 1998 No 133
d. Australian Privacy Principles
e. Federal Mandatory Data Breach Notification
f. State Records Act 1998 No 17

Intellectual property rights

(274) Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights and on the use of proprietary software products.

(275) All computer programs and program documentation owned by the University must include appropriate copyright notices.

Protection of records

(276) University records must be protected from loss, destruction, and falsification. Refer to the Records Management Policy, Privacy Management Plan and the Information Technology Procedure - Personal Data Breach.

Information security reviews

(277) The University must conduct information security reviews to ensure that information security controls are implemented and operated in accordance with the University's policies and procedures.

Independent review of information security

(278) The University's approach to managing information security and its implementation (e.g. control objectives, controls, policies, processes and procedures) should be reviewed independently at planned intervals or when significant changes occur.

Compliance with security policies and standards

(279) The University must ensure that all security procedures within their areas of responsibility are carried out correctly. Areas within the University that must be subjected to regular reviews to ensure compliance with security policies, procedures and standards include, but are not limited to:

a. information systems
b. system providers
c. management
d. users, and
e. custodians of information and assets.

(280) Variances from generally accepted information system control practices must be noted and promptly initiated for corrective action.

Technical compliance review

(281) Technical compliance should be reviewed with the assistance of automated tools which generate technical reports for subsequent interpretation by technical specialists. Alternatively, manual reviews by experienced system engineers supported by appropriate software tools may be performed.

(282) Any technical compliance reviews such as penetration tests or vulnerability assessments should only be carried out by competent authorised users and/or under the supervision of such users.

Information security management system (ISMS) performance monitoring process

(283) The operation of the ISMS will be monitored in accordance with the University ISMS performance monitoring process.

Benchmarking

(284) Cyber security benchmarking should be conducted to ensure that the University's cyber security posture is aligned with the evolving threat landscape and sector opportunities.

(285) With reference to industry benchmarks, frameworks, standards and best practices, the University will identify gaps and vulnerabilities in deployed security controls and develop remediation plans to address these issues as part of an ongoing continuous improvement program.

(286) Benchmarking reviews will be carried out by competent authorised parties and will include the following elements:

a. Assessment of current cyber security controls and procedures against sector peers.
b. Identification of gaps and vulnerabilities.
c. Development of remediation plans.
d. Tracking of progress and reporting on results.

Section 5 - Glossary

(287) This guideline uses terms defined in the Information Technology Policy, as well as the following:

a. Administrative privileges – means any feature or facility of an information system that enables the user to override system or application controls.
b. Asset custodian – means an authorised user with responsibility and ownership of Information and Communication Technology (ICT) assets as identified and listed in the University's asset registers.
c. Business critical assets – include:
    i. information
    ii. software
    iii. physical assets
    iv. services.
d. DIT Change Advisory Board (CAB) – ensures that all requested IT changes are thoroughly checked and assessed from both a technical and business change risk/impact perspective. No change can be implemented in any production environment without appropriate CAB approval.
e. Cloud platform – means on-demand access of hosted applications, systems and infrastructure in various forms and models, including:
    i. Infrastructure as a Service (IaaS)
    ii. Platform as a Service (PaaS)
    iii. Identity as a Service (IDaaS)
    iv. Software as a Service (SaaS)
    v. Integration platform as a Service (IPaaS).
f. Computer media - includes:
    i. tapes
    ii. disks
    iii. cassettes
    iv. faxes
    v. removable media
    vi. printed reports.
g. Computer system(s) – means any University system used for the processing of information, either within the University premises, or at an off-site location. This includes private and/or third-party equipment, if such equipment is used to access University information.
h. Controlled area – means any area or space on University premises to which general or public access is not available at that time. This may be characterised by signs, locked doors, fences, boom-gates, sentinel tape, or be defined by the instruction of a Campus Security Officer or designated member of staff.
i. Cryptography key – means a string of bits used by a cryptographic algorithm to transform plain text into unreadable format or vice versa.
j. Crypto period – means the time for which a cryptography key is valid.
k. Custodian – means the senior responsible officer of the group that administers and operates that information asset or system.
l. Data asset register – includes:
    i. data assets
    ii. security classification (e.g. unclassified, sensitive, public)
    iii. custodianship

iv. location
v. relative value
vi. importance.

m. Failover – means a procedure by which a system automatically transfers control to a duplicate system or redundant system when it detects a fault or failure.
n. Granularity – means the frequency with which data is backed up. Data that is present for less than this time period may not be captured by the backup process and hence may not be recoverable.
o. Information security - encompasses:
    i. ICT security policies
    ii. organisation of information security
    iii. ICT asset management
    iv. information security compliance obligations
    v. information security components of human resources management
    vi. ICT communications and operations management
    vii. information security components of business continuity management
    viii. ICT services access control
    ix. ICT security incident management
    x. ICT systems acquisition, development and maintenance
    xi. ICT asset physical and environmental security.
p. Infrastructure as a Service (IaaS) – means cloud service capability provided to users to provision processing, storage, networks, and other fundamental computing resources where users can deploy and run arbitrary software. This may include operating systems and/or applications. Users do not manage or control the underlying cloud infrastructure, typically managed by the Cloud Service Provider.
q. Hypervisor – means software, firmware or hardware that creates and runs virtual machines.
r. Malware – means malicious software. An umbrella term used to refer to a variety of forms of hostile or intrusive software.
s. Managed device – means a University supplied personal computing or mobile device registered to the University network with standard University software installed and updated by the Division of Information Technology.
t. Multi-tenancy – means use of the same resources or application by multiple users (e.g. tenants) that may belong to the same or different organisations. Impacts of multi-tenancy may or may not include the presence of data and/or trace of operations from multiple users of the resource and/or application. Multi-tenancy impacts will vary depending on the cloud service model (e.g. IaaS, PaaS, and SaaS).
u. Need to know – means access to the sensitive information necessary for the conduct of an individual’s official duties.
v. Network services – include:
    i. messaging (e.g. email, instant messaging)
    ii. file transfer
    iii. interactive access
    iv. application access.
w. Non-managed personal computing/mobile device - is a personal computing or mobile device not registered to the University network. Setup is as received out of the box from the vendor. Includes telephony devices connected to the cellular network.
x. Personal identification number (PIN) - means a secret number (usually four to six digits in length) known only to an individual. Used to confirm identity and gain access to an Information and Communication Technology (ICT) system.

y. Platform as a service (PaaS) – means cloud service capability provided to users to deploy user-created and/or acquired applications developed using programming languages, libraries, services and tools, as supported by the Cloud Service Provider.

z. Principle of least privilege – means an authorised user is given access only which is essential to perform the needs of their work role.

aa. Privileged access – means the ability to perform an action (e.g. administrative functions) outside of a user's day to day job function, using a secondary account.

ab. Resources – means information technology support staff, technologies and supporting infrastructure owned or maintained by the University.

ac. Software as a service (SaaS) – means cloud service capability provided to users to use a Cloud Service Provider's applications running on cloud infrastructure. Such applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email) or a program interface.

ad. System custodian – means university executive staff with responsibility and ownership of information or Information and Communication Technology (ICT) assets as identified and listed in the University's Applications Portfolio, or the Primary Budget Centre Manager responsible for non-listed systems.

ae. Third party service provider (TPSP) – means a professional organisation engaged by a company to provide services for and in the name of the organisation to their clients.

Status and Details

Status	Current
Effective Date	24th July 2023
Review Date	24th July 2026
Approval Authority	Chief Operating Officer
Approval Date	24th July 2023
Expiry Date	Not Applicable
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Mark Duffy Director, IT Infrastructure and Security
Enquiries Contact	Division of Information Technology