Computer and Network Security Procedure

Section 1 - Purpose

(1) This Procedure specifies the standards for cyber security protection for the University's computer and network resources in accordance with the Cyber Security Policy.

Scope

(2) This Procedure applies to:

a. all computer and network resources operated by, or on behalf of, the University (including its controlled entities); and
b. all individuals, including third parties, involved in deploying and supporting computer and network resources for use by the University.

Section 2 - Policy

(3) Refer to Cyber Security Policy.

Section 3 - Procedures

RESPONSIBILITIES AND REQUIRED ACTIONS

(4) It is the responsibility of all Macquarie Information Technology (IT) staff to understand the requirements of the University's Information Security Management System (ISMS) documented in this Procedure, specifically requirements relating to:

a. Access Control;
b. Building Secure Systems;
c. Secure Development;
d. Vulnerability Management;
e. Vulnerability Risk Assessment;
f. Network Security;
g. Encryption;
h. Logging and Monitoring; and
i. Decommission and Destruction.

Part A - Access Control

(5) The University's IT resources must be configured to only permit authorised access to system functions and information.

Accounts

(6) The University will employ processes and systems to ensure the correct provisioning, review and removal of system and application accounts. A secure account management processes must be documented and followed to ensure:

a. all individuals requiring access are provided with unique accounts that are named so that the account owner can be identified;
b. approvals from an authorised staff member are obtained and recorded for each account requested;
c. University staff are only provided with the access required to perform their job responsibilities;
d. account privileges are restricted or removed if a staff member changes job roles in alignment with their new job responsibilities;
e. access to the University email system is removed for accounts of academic staff three months after they leave the University's employment;
f. access is removed for accounts for all other systems on the day they leave the University's employment;
g. accounts are periodically reviewed to ensure access that is no longer required is revoked;
h. accounts are disabled if unused for 180 days; and
i. security events generated by user activity are logged to a central log repository.

Passwords

(7) The University's systems must enforce the following password restrictions. Passwords must:

a. be at least eight characters in length;
b. contain three of the character types: uppercase letters, lowercase letters, numbers, or special characters;
c. not be the same as the previous five passwords chosen for that account;
d. not be able to be changed more than once a day;
e. be protected by a one-way hashing algorithm when stored; and
f. not be displayed when they are entered during the login process.

(8) Systems must also employ measures to ensure that passwords are not guessable through the login interface. System must ensure that:

a. accounts are locked out for 30 minutes after 15 consecutive failed login attempts.

(9) Access to applications that contain confidential, or highly sensitive information require multi-factor authentication, when accessed from off-campus locations.

Access Warning

(10) A message that discourages unauthorised access and notifies the user of activity monitoring must be displayed before a user attempts to logon to a system or application.

(11) For computer systems console access and network devices:

> WARNING! This system belongs to Macquarie University. AUTHORISED ACCESS ONLY.
>
> Access to this system is restricted to authorised users only. Actions performed by users on this system are logged and monitored. Activities conducted on this system that contravene the University's policies and procedures will be reported to the relevant authorities.

(12) For internal applications:

> This application is operated by Macquarie University. Access to this application is restricted to authorised users only. Actions performed by users within this application are logged and monitored. Misuse of this application and its facilities will be reported to the relevant authorities.

Central Authentication

(13) Where technically possible, all systems and applications must authenticate users to a central authentication provider. The following controls must be in place:

a. Use strong encryption for the transmission of username and password during the authentication process (e.g. Kerberos or LDAP over SSL) in accordance with the encryption requirements under the Encryption section of this Procedure.
b. Pass-through authentication (single sign-on) is permitted unless the application facilitates access to “Highly Sensitive” information.
c. User sessions must expire after 20 minutes of inactivity if facilitating access to “Highly Sensitive” information.

Database ACCESS

(14) Databases typically store large quantities of data. Access to databases containing production information must be strictly controlled:

a. Non-production applications and databases must not contain production data.
b. The System Administrator (SA) account must only be used in the case of an emergency; all direct access to databases must be conducted with the users unique ID.
c. Applications that integrate with a database must be provided with a unique application account that is only used for interaction with the database by the application.
d. Applications that allow users to access data directly from a database must log the identity of the user within user activity logs for data create, read, update, or delete activities.

Privileged Accounts and Passwords

(15) Administrator and super user accounts that have access to large quantities of information or privileged system functions, represent a significant risk to the University. Accounts that provide privileged access are subject to the following additional security requirements:

a. must be approved by an authorised University officer or employee;
b. must be assigned to an individual and be named so that the account owner can be identified;
c. must enforce system access based on the role assigned to the individual;
d. initial system access must be restricted to normal user access with a requirement to escalate privileges for privileged information access or functions; and
e. must utilise multi-factor authentication.

(16) Privileged generic accounts, such as root, Administrator or enable, exist on almost all computers and network devices. Passwords for such accounts must:

a. only be used in the case of an emergency;
b. be reset to a randomly generated password of at least 16 characters at build time and at any time the password is communicated between staff members or third parties in the case of an emergency;

c. be stored in a secure digital format protected by strong encryption;
d. only be accessible by the minimum number of support staff required;
e. not be communicated in the same communication medium as the system name and account name; and
f. not be sent by email or computer based instant message technology. SMS, iMessage, or verbally over the phone is permitted.

Temporary Passwords

(17) Temporary passwords are required for the initial set-up of user accounts and the resetting of passwords for existing accounts. Temporary passwords can be sent via email but must:

a. conform to the same complexity and length requirements as described under the Passwords section of this procedure;
b. be unique to each occurrence of a new account or password reset request;
c. require the user to change the password on next login; and
d. expire after 24 hours.

Console Access

(18) Access to a system console constitutes access to the operating system's command line interface or graphical user interface. System consoles typically allow access to privileged functions and other applications and systems that the user is connected to. Console access must:

a. require re-authentication after 20 minutes of inactivity; and
b. not be directly accessible from the internet with a single factor of authentication.

System-to-System Accounts

(19) Connections between systems typically constitute privileged access for data transfer or automated system interactions. Credentials for system-to-system connectivity should have minimised handling only to initiate the connection between systems. System-to-system accounts must adhere to the following requirements:

a. must not be used by individuals for day-to-day operations;
b. must be either certificate based or consist of a password of at least 16 characters;
c. must contain three of the character types: uppercase letters, lowercase letters, numbers, or special characters;
d. can be set to never expire; and
e. must be protected by strong encryption or restrictive file system permissions when stored (only permit access to the required application accounts).

Service and Application Accounts

(20) Service accounts are used by application and system services to perform automated operations. Service accounts can represent a risk to the University if not configured correctly. Service accounts must:

a. be configured not to permit remote or direct console login;
b. not be a root or administrator account for the underlying operating system;
c. only be provided with the permissions required to perform its operations;
d. have unique passwords (no identical passwords for service accounts across multiple systems);
e. be named after the service or application that utilises the account;
f. only be used for the purposes related to running or configuration of the relevant service or application; and

g. be set with a randomly generated password of at least 16 characters (default passwords must be reset).

Access Via Mobile Devices

(21) Tablets and smartphones are typically not bound to a physical location and are exposed to meetings and locations with third parties and members of the public. Personal and University supplied mobile devices used to access the University's systems or information must:

a. be protected by a PIN or password at least four characters long;
b. require re-authentication after five minutes of inactivity; and
c. have the ability to be remotely wiped.

Part B - Building Secure Systems

Secure Build and Configuration

(22) All computer systems built and configured for the purposes of University use, are subject to the following requirements:

a. must be assigned a system owner and be registered in an asset database with system owner's name, business owner's name, computer name, IP address, and business purpose;
b. must be located in an appropriate network zone in accordance with the Network Security section of this Procedure; and
c. must be built in accordance with an applicable security baseline that includes the following configuration items:
    i. The system clock must be synchronised with a trusted time provider.
    ii. Must have unneeded services and software packages disabled or removed.
    iii. Must have unneeded accounts removed, default credentials changed, and anonymous access disabled.
    iv. Must be configured to deny network, shell, console, and file system access unless specifically permitted.
    v. When commissioned into production, must have the relevant security patches applied that address security vulnerabilities for the deployed version.
    vi. Must have media and network drive auto-play functions disabled.
    vii. Must restrict privileged actions as well as access to configuration, log, and system files to administrator accounts only.
    viii. Must log security events and privileged actions to a central log server in accordance with the logging requirements under the Logging and Monitoring section of this Procedure.
    ix. Must be configured with a personal firewall if operating on premises that are not owned or operated by the University.
    x. Must enforce secure user access in accordance with the Access Control section of this Procedure.

Protection from Viruses and Malware

(23) If the system runs a Microsoft Windows-based operating system, performs file transfer services, or is a public-facing web server, the system must:

a. have centrally managed, real-time antivirus software installed;
b. initiate an antivirus signature update at least every four hours; and
c. have locally mounted disks scanned by antivirus software on a weekly basis.

Computer Systems That Handle Highly Sensitive information

(24) To comply with regulations and industry standards, computer systems that handle Highly Sensitive information are required to comply with the following additional security requirements:

a. Application whitelisting must be used to restrict application and script execution to only those folders or directories required to perform the business function.
b. If not located in a locked cabinet within a datacentre, must have USB ports, floppy disk drives, and optical drives disabled.
c. Must be monitored by change detection software that monitors critical system files and logs exception events to a central log server in accordance with the logging and monitoring requirements under the Logging and Monitoring section of this Procedure.
d. Must log all data-level access to “Highly Sensitive” information to a central log server.

(25) The Information Classification and Handling Procedure provides further information about staff and student responsibilities for handling Highly Sensitive information.

Part C - Secure Development

Security testing in the Software Development Life Cycle

(26) Following a documented and mature software development life cycle allows developers to incorporate tests for security issues early in the development process. Software written for use by the University should follow a standardised development life cycle that incorporates at least two security tests. For example, tests may take the form of a manual code review, static analysis or penetration test.

Web Application Development

(27) Web applications are commonly exposed to a large number of untrusted users. Developers must take additional precautions when developing web applications, including:

a. implement protection from the OWASP Top 10 Web Application Security Risks.;
b. scan for, and address vulnerabilities in accordance with the vulnerability management requirements under the Vulnerability Management section of this Procedure, after every change to the code or configuration of production software;
c. if externally accessible, segment the web application into presentation, application, and database zones in accordance with network security requirements under the Network Security section of this Procedure; and
d. restrict exposure to non-production applications to internal networks only.

Part D - Vulnerability Management

Vendor Security Advisories

(28) Software vendors regularly publish advisories notifying customers of their software that security vulnerabilities have been identified. Staff responsible for maintaining systems or applications must subscribe to the relevant advisories. This includes the following responsibilities:

a. Staff responsible for supporting computer system infrastructure (desktops and servers) must subscribe to vulnerability advisories for operating systems and virtual server platforms in use by the University.
b. Staff responsible for supporting network infrastructure must subscribe to vulnerability advisories for network devices and network management systems in use by the University.

c. Staff responsible for supporting applications and databases must subscribe to vulnerability advisories for applications and database infrastructure in use by the University.
d. Staff responsible for supporting security infrastructure (e.g. firewalls, antivirus, antispam, encryption, and VPN systems) must subscribe to vulnerability advisories for security infrastructure in use by the University.
e. Security operations staff must subscribe to general security advisories from local and international authorities (e.g. AusCERT, US CERT, Stay Smart Online).

(29) Security vulnerabilities for software and systems in use by the University must be assessed for criticality. Alerts rated as high or critical must be actioned in accordance with the Vulnerability Risk Assessment section of this Procedure to ensure that University systems are patched as needed.

Part E - Vulnerability Risk Assessment

(30) A risk assessment must be conducted on vulnerabilities as they are published or advised by software and infrastructure vendors.

(31) The risk rating of a particular vulnerability is calculated by assessing the risk factors in Table 1: Risk Factors.

Table 1: Risk Factors

Risk factor	Risk rating = 1	Risk rating = 2	Risk rating = 5
Exposure	Local subnet	Campus network	Public access
Asset at risk	Public	Controlled	Confidential
Exploitation	Non-trivial	Not-public	Demonstrable
Execution	User interaction	Authenticated	Unauthenticated
Scope	1-5 systems	6-10 systems	> 10 systems

(32) The following Risk Rating calculation is then used to determine the risk that a vulnerability poses to the University:

> Risk rating = Exposure factor + Asset at risk factor + Exploitation factor + Execution factor + Scope factor

Table 2: Risk Rating – severity and notification and response requirements

Risk Rating	Severity	Description	Notification	Response
> 17	Critical	The exploitation of the vulnerability presents an imminent threat with the potential of: 1. Exposing confidential information to unauthorised parties 2. Disrupting the operation of critical systems 3. Damage to the University's reputation	CIDO	Resolved in 48 hours
10 - 16	High	The exploitation of the vulnerability presents a likely threat with the potential of: 1. Exposing bulk controlled information to unauthorised parties 2. Disrupting the operation of important systems	IT Directors and Information Security Manager	Resolved within one month

Risk Rating	Severity	Description	Notification	Response
1 - 16	Medium - Low	The exploitation of the vulnerability presents a likely threat with the potential of: 1. Exposing a small amount of controlled information to unauthorised parties 2. Disrupting the operation of systems with limited users	System Owner and Information Security Manager	Resolved during normal patching cycle

Software Patching Cycles

(33) Software in use on University desktops, servers and network devices must reviewed for security patching on a regular basis. The frequency of review is based on the following exposure levels:

a. Externally exposed (allows direct interaction from internet) – monthly review;
b. Authenticated or internal access only – quarterly review.

(34) Timeframes for patching depend on the severity of the vulnerability determined by the risk assessment framework defined in the Vulnerability Risk Assessment section of this Procedure.

Part F - Network Security

Secure Network Environments

(35) All network environments owned, maintained, or operated by the University are subject to the following requirements:

a. “Confidential” data, “Highly Sensitive” data and authentication credentials must be protected in transit by strong encryption in accordance with encryption requirements under the Encryption section of this Procedure.
b. Firewalls must only allow the ports required for the business function and deny all other traffic.
c. All network zones must be protected from the internet and third-party environments by a dedicated firewall system.
d. Computer systems that require direct connection to external locations (inbound and outbound) must be located in a DMZ..
e. All inbound traffic from external locations to internal systems (non-DMZ) must pass through a proxy or bastion host located in a DMZ that performs protocol inspection or conversion.
f. Internet access provided by the University must be filtered to prohibit access to malicious or potentially dangerous sites.
g. The firewall system protecting a computer system in the DMZ must not be configurable from the computer system it is protecting.
h. Non-production environments must be separated from production environments by a dedicated firewall system.
i. Key chokepoints between network zones must be monitored by intrusion detection and prevention systems that notify the Macquarie IT Cyber Security when an attack or violation of policy is detected.
j. Console access to systems must not be directly accessible from the internet with a single factor of authentication.

Web Application Environments

(36) Network environments that host internet facing web applications are particularly susceptible to attacks from malicious parties. Special segmentation and traffic rules that protect web applications and limit exposure in the event of an attack are required. Web application environments must adhere to the following requirements.

a. Must reside in at least a two-tier network architecture (application and database).
b. Servers in the database zone must not be permitted to initiate connections directly with the application zone.
c. Servers directly involved in hosting internet-facing web applications must have outbound traffic to the general internet blocked.

Remote Access for Privileged Users

(37) Remote access allows trusted personnel to access the University's recourses from remote locations. Strong authentication is required to ensure that access is authorised and access beyond a business need or staff employment is revoked. It is required that:

a. remote access is authenticated by multi-factor authentication;
b. remote access is removed immediately when no longer required;
c. remote access traffic must be protected by strong encryption; and
d. if provided for a specific task, remote access should be limited to the time period allocated for the task.

Network Device Security

(38) Switches, routers, and firewalls facilitate the transmission of University information and access to all University applications. All network devices must be configured to protect against unauthorised access and malicious attack. Requirements are that:

a. unneeded accounts are removed and default credentials changed;
b. unneeded services and software packages are disabled or removed;
c. the system clock is synchronised with a trusted internal time source;
d. secure user access is ensured in accordance with access control requirements under the Access Control section of this Procedure;
e. security events are logged to a central log server;
f. when commissioned into production, must have the relevant security patches applied that address security vulnerabilities for the deployed software version;
g. a patching cycle is maintained in accordance with the Vulnerability Management section of this Procedure; and
h. the network device is located in a physically secure area that protects against tampering or theft.

Firewall and Network Change Approval

(39) Firewall rule changes must be reviewed and approved by Macquarie IT Cyber Security if they meet one or more of the following conditions:

a. permit traffic to or from external (internet or third party) locations;
b. permit traffic between production and non-production environments;
c. permit a large number of source or destination addresses (greater than 10);
d. permit all source or destination protocols (an "ANY" rule);
e. permit a broad range of source or destination protocols (greater than a range of 20 ports);
f. establish a new network path to an external party;
g. use protocols that pass credentials or data in clear text (SNMP, POP3, IMAP, LDAP, FTP, TFTP, Telnet, rexec, rlogin, rsh);
h. use protocols that are known as an avenue for computer worms (SMB/CIFS TCP445 & TCP139, MS-RPC TCP135, RDP TCP3389); and
i. facilitate remote control of computers (RDP TCP3389, VNC TCP5500 TCP5800 TCP5900, pcANYWHERE TCP5631

UDP5632).

Part G - Encryption

Approved Encryption Methods

(40) Protection of information with cryptography or hashing must employ the following algorithms and minimum key lengths.

(41) Symmetric encryption:

a. Advanced Encryption Standard (AES) – 128-bit keys
b. Triple Data Encryption Standard (DES) – 168-bit keys

(42) Asymmetric encryption:

a. Rivest, Shamir and Adlemen (RSA) – 2048-bit keys

(43) Hashing:

a. Secure Hashing Algorithm 2 (SHA-2) – 256-bit digest length

(44) Password encryption:

a. Password-Based Key Derivation Function 2 (PBKDF2)
b. Bcrypt
c. Argon2

TLS Certificates, encryption and protocols

(45) Application access and data transfers that are secured by TLS (also known as SSL) must be conform to the criteria below:

a. All versions of SSL (1, 2 & 3) must be disabled;
b. The TLS version must be 1.2 or above;
c. Certificates must be signed with SHA-256 certificates and certificate chains;
d. Asymmetric key length must be 2048 or higher; and
e. If Diffie-Hellman is used for key exchange, a 2048-bit group must be used.

(46) Additional validation is required for internet-facing websites:

a. Certificates must be signed by a well-established commercial certificate authority; and
b. Certificates must have, at most, a three-year validity period.

(47) For system-to-system interfaces:

a. Certificates may be self-signed ;and
b. Certificates may be valid for up to six-years.

Secure Encryption Key handling

(48) Keys used for encryption must be protected when transmitted or stored:

a. Keys must only be provided to those who have a business need to handle the keys.
b. Keys must be protected by strong encryption during delivery to technical staff.
c. Application keys or private keys for scripts, needed at system startup, must be stored in a location with read permissions only for the application or script user. All other permissions must be removed.
d. Passwords used to encrypt keys must be at least 12 characters and must contain three of the character types: uppercase letters, lowercase letters, numbers, or special characters.
e. Passwords to decrypt keys must not be sent by email or computer based instant message technology. SMS, iMessage, or verbally over the phone is permitted.
f. Key encrypting keys must be stored separately to data encrypting keys.
g. Keys must be stored in a single encrypted location that is regularly backed up to an encrypted repository.
h. Keys must be replaced if they are no longer considered strong by industry standards or if there is a suspicion of exposure to unauthorised parties.

Part H - Logging and Monitoring

(49) The University will implement a practical and appropriate level of logging and monitoring to ensure that malicious events are identified and there is sufficient information to investigate and identify the origin of incidents.

Security events to be Logged

(50) Successful and unsuccessful attempts to initiate the following events must be logged:

a. account log-on and log-off;
b. password resets;
c. account lockouts;
d. user and group creation, modification, or removal;
e. privilege escalation;
f. actions taken by privileged users (root, sa, Administrator, enable);
g. modification of system configuration;
h. access to “Highly Sensitive” information (refer the Information Classification and Handling Procedure for a definition) ;
i. modification of security logs;
j. starting and stopping of system security services (e.g., logging, antivirus, file change detection, firewall);
k. system or application errors and warnings; and
l. activities invoked by scheduling systems.

Security event Log Contents

(51) Security logs must include enough information to identify the nature of the events as well as to attribute the event to an individual or system. To adequately identify the origin of events and provide insight into an incident, security logs must include:

a. user account name;
b. date and time stamp;
c. origin of the event (IP address or DNS name);
d. description of the event including the affected system object, file, or user;
e. system in which the event occurred; and
f. indication of activity success or failure.

Central Logging

(52) Where possible, applications and systems must send logs in real-time to the central security logging and monitoring system. Logs sent to the central system must:

a. be retained for immediate access for one month; and
b. be monitored for malicious events by an automated log correlation and alerting tool.

Part I - Decommission and Destruction

(53) University records must be retained in accordance with the Records and Information Management Policy. Information that is not required to be retained for regulatory or University purposes on printed material or in a digital format must be securely destroyed so that the information is not able to be recovered by unauthorised parties. Destruction of University records must be approved by an authorised staff member and documented as a record itself.

System Decommission

(54) Systems that are decommissioned must have their network and IT support references removed. This includes removing:

a. associated firewall rules and IP access control lists;
b. VPN profile associations;
c. forward and reverse DNS entries;
d. entries in support databases such as the CMDB;
e. system specific domain-level service accounts; and
f. deletion of virtual machines and associated virtual disks.

Destruction of Printed Material

(55) Printed documents must be destroyed by using secure facilities provided by the University:

a. by depositing in a locked secure destruction bins supplied by a AAA certified National Association for Information Destruction organisation; or
b. By use of a DIN 66399 security level P-4 to DIN 66399 security level P-7 document shredder.

Destruction of Optical Media

(56) Optical media can contain significant amounts of information and must be destroyed when no longer needed. The following are acceptable methods of destroying optical disks:

a. by safely cutting into four similar sized pieces with a pair of scissors;
b. by use of a DIN 66399 security level P-4 to DIN 66399 security level P-7 document shredder that has CD and DVD shredding capabilities; or
c. by disposal through a AAA certified National Association for Information Destruction organisation (a certificate of destruction must be obtained).

Repurposing Equipment

(57) Systems that are being repurposed must have their storage devices wiped before being deployed into their new function. The wiping procedure must adhere to the following:

a. include at least a three-pass zeroing of all addressable locations; and

b. a screenshot must be captured of the successful wipe operation and provided to Macquarie IT Cyber Security.

Equipment Disposal by a Third Party

(58) Systems that are being decommissioned and passed on to a third party for disposal must have their storage devices securely wiped either before providing to the third party or by the third party with adequate proof of destruction. If the third party is performing the data destruction the following requirements must be met:

a. The third party must be AAA certified with the National Association for Information Destruction.
b. The third party must provide a certificate of destruction for each storage device provided.
c. The serial number of each device must be catalogued before destruction and listed in the certificate of destruction.

Wiping of Network Devices

(59) Network devices contain information relating to the University's internet network environment and communications links. In some cases, network devices contain VPN passwords, encryption keys, and network configuration details. Information contained on network devices must be securely wiped if being decommissioned, disposed of, or repurposed.

a. Network device configuration must be reset to the factory default in accordance with the manufacturer's instructions
b. Hard disks contained within network devices must be destroyed in accordance with the Decommission and Destruction section of this Procedure or securely wiped.

Section 4 - Guidelines

(60) Nil.

Section 5 - Definitions

(61) The following definitions apply for the purpose of this Procedure:

a. DMZ is a short name for a "demilitarised zone". A DMZ consists of a network zone within the University network that sits between an external and untrusted network zone and an internal protected network zone. DMZ networks typically hold externally accessible systems that are screened or filtered from access to internal systems.
b. Malicious or dangerous sites are external network locations that are known to host malware or deceptive content such as fake websites used for phishing. These sites may be able to infect a computer with viruses or steal the usernames and passwords.

Status and Details

Status	Current
Effective Date	29th April 2021
Review Date	29th April 2024
Approval Authority	Vice-President, People and Services
Approval Date	29th April 2021
Expiry Date	Not Applicable
Responsible Executive	Nicole Gower Vice-President, Professional Services
Responsible Officer	Jonathan Covell Chief Information and Digital Officer
Enquiries Contact	Shad Thakkar Chief Information Security Officer Information Technology