Computer and Network Security Policy

Section 1 - Purpose

(1) This Policy outlines how IT Resources and user accounts are to be secured in accordance with the Cyber Security Policy.

Scope

(2) This Policy applies to all staff employed by Macquarie University and its controlled entities and Affiliates who:

a. have access to IT Resources; and
b. are responsible for implementing and managing IT Resources.

Background

(3) Macquarie University (the University) is committed to maintaining a secure technology environment and as such, has established requirements to secure the University's IT Resources. Establishing these requirements aims to decrease the likelihood of negative consequences impacting the Confidentiality, Integrity and Availability of IT Resources.

Section 2 - Policy

General Access Management

(4) User access provisioning, account management, and password allocation should only be performed by the Central IT team, in accordance with approved operational procedures.

(5) Access to IT Resources should be controlled through a central identity management platform (e.g., Active Directory (AD) group membership).

(6) Access to applications should be facilitated via Single-Sign-On (SSO), where possible.

(7) User accounts must be configured with Multi Factor Authentication(MFA) and User accounts should be unique to an individual.

(8) A user access provisioning process should be implemented to assign or revoke access to IT Resources. User access should be:

a. assigned in accordance with the principle of least privilege and segregation of duties;
b. assigned after formal approval from the user's manager or relevant Business Owner (or authorised delegate). Additionally, Privileged User access must also be reviewed by the Business Owner (or authorised delegate) and the Cyber Security team before being provided;
c. uniquely identifiable and accountable to a single individual;
d. removed on the same day when no longer required (e.g., upon termination, role change, or responsibility

change); and

e. configured with an expiry date for Third-Party accounts that aligns with the user's contract end date.

(9) Systems under organisational control must enforce account lockout controls to mitigate brute-force and credential guessing attacks. Specific lockout parameters (including attempt threshold, lockout duration, and counter reset) are defined in the standards/baseline and approved by the cyber security function.

(10) User access permissions should be reviewed for suitability by the Business Owner (or authorised delegate) or Cyber Security team, at the following cadences:

a. Standard User accounts: at least annually; and
b. Privileged User accounts: at least every six months.

(11) User access permissions should also be reviewed in response to one of the following:

a. a user's role or position changes;
b. an incident (e.g., account compromise or data breach); or
c. a disciplinary breach (e.g., breach of a relevant Policy).

Account Management

(12) Access management systems must be configured to 'deny by default' unless explicit access is granted.

(13) Both privileged and unprivileged access to IT Resources should be automatically disabled after 90 days of inactivity.

(14) Privileged Users should maintain a Standard User account for their day-to-day non-privileged work and use a specific Privileged User account for any tasks that require elevated privileges.

(15) Elevated/higher privileges should not be granted to a Standard User account.

(16) The owner of a user account will be held responsible for all actions undertaken by the account.

(17) The use of shared user accounts must be documented and an owner must be assigned to each shared user account.

Password Management

(18) Where available, University approved password managers should be used.

(19) IT Resources that manage/enforce passwords should be configured to enforce the following requirements:

Requirement	**Settings**
Minimum Password Length	Standard User accounts (8 characters); and Privileged User accounts (16 characters).
Password Expiry	Standard and Privileged User accounts (1 year).
Password History	5 previous passwords.

Requirement	Settings
Password Complexity	Passwords must contain: at least one uppercase or lowercase character (e.g., A – Z or a – z); at least once number/digit (e.g., 1 – 9); and at least one special character (e.g., #, %, $). Passwords must not contain: Commonly used words or commonly used passphrases; and Part of a users' username, first name, or last name.

(20) Privileged account passwords must be randomly generated at build time and at any time the password is communicated.

(21) Temporary passwords should adhere to the same requirements detailed in clause 19 and be set to expire after 24 hours.

(22) Passwords must be changed in response to one of the following:

a. a user logs on for the first time; or
b. if it has been or is suspected of being compromised.

(23) Password resets should be logged to provide an audit trail for any future investigation.

(24) Passwords should be securely stored within a University approved password manager.

(25) Password generated by applications/systems should be shared via a secure and approved distribution method.

(26) Passwords must not be shared with another individual.

(27) Scripts, code, or macros should not contain passwords.

(28) Passwords used for encryption keys should comply with the same minimum requirements as required by the Privileged User Accounts.

(29) Passwords used to decrypt keys should only be verbally shared with authorised users.

Network Security

(30) IT Resources should be documented within an asset register, inclusive of the following information:

a. System Owner's name;
b. Business Owner's name;
c. asset name/identifier;
d. Internet Protocol (IP) address;
e. criticality rating;
f. confidentiality rating; and
g. business purpose.

The asset register will be maintained by IT, with input from relevant business owners to ensure completeness and accuracy.

(31) IT Resources not approved by the University should not be connected to the University's corporate network.

(32) IT Resources should be onboarded, maintained and offboarded in accordance with a defined asset management process.

(33) Networks should be segmented and network zones classified different from public.

(34) Network zones should be protected from the internet and Third-Party environments by perimeter controls including but not limited to a firewall and Access Control Lists (ACLs).

Malware

(35) IT Resources attached to the University's network must have anti-malware software installed. The software must:

a. be active;
b. be scheduled to perform checks at regular intervals;
c. have its definition files kept up to date; and
d. initiate an anti-malware signature update at least every four hours.

(36) Malware-infected IT Resources must be removed from the network until it is verified as virus-free.

(37) All encrypted artefacts must be scanned for malware after decryption and before execution.

(38) All artefacts obtained or downloaded must be scanned for malware before executing.

(39) Locally mounted disks should be scanned by anti-malware software on a weekly basis.

Encryption

(40) University information should be encrypted in-transit and at-rest, in accordance with the Australian Signal Directorate (ASD) Approved Cryptographic Algorithms.

(41) Internet-facing website validation should adhere to the criteria below:

a. certificates should be signed by a well-established commercial certificate authority; and
b. certificates should have at most, a 200 day validity period.

(42) System-to-system interfaces should adhere to the criteria below:

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

(43) Encryption keys must adhere to the criteria below:

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 in-transit;
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:
    i. all other permissions should be removed.
d. Key Encrypting Keys (KEKs) should be stored separately to Data Encrypting Keys (DEKs);
e. keys should be stored in a single encrypted location and regularly backed up to an encrypted repository; and
f. keys must be replaced if they are no longer considered strong by industry standards or if they are suspected of being compromised.

IT Resource Decommissioning

(44) University records must be retained in accordance with the Records and Information Management Policy.

(45) Information that is not required to be retained for regulatory or University purposes on printed material or in a digital format should be securely destroyed so that the information is not able to be recovered by unauthorised parties.

(46) Destruction of University records should be approved by authorised staff and documented.

(47) Printed documents should be destroyed by using secure facilities provided by the University by:

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

(48) Optical media and hard disks that contain University information should be securely deleted/wiped before being repurposed.

(49) Optical media and hard disks should be physically destroyed before being disposed, by disintegration, incineration, pulverising, shredding, melting or through a AAA certified National Association for Information Destruction organisation, with a certificate of destruction.

(50) Decommissioned, disposed and repurposed IT Resources must have:

a. their storage devices/media securely deleted/wiped, by either:
    i. the University; or
    ii. a AAA certified National Association for Information Destruction organisation, with a certificate of destruction;
b. their serial numbers recorded within a register;
c. their settings/configurations reset to factory default;
d. associated firewall rules and IP access control lists removed;
e. Virtual Private Networks (VPN) profile associations removed;
f. forward and reverse Domain Name Service (DNS) entries removed;
g. entries in support databases removed (e.g, Configuration Management Database);
h. system specific domain-level service accounts removed; and
i. virtual machines and associated virtual disks deleted.

Compliance and Exemptions

(51) Any exemption from this Policy must be sought from the Chief Information Security Officer (CISO).

(52) Breaches of this Policy will be managed in accordance with the applicable provisions of the Staff Code of Conduct and other relevant policy instruments.

Section 3 - Procedures

(53) IT Resources must be built/configured in accordance with, but not limited to, the following requirements:

a. be synchronised with a common trusted time source;
b. have unneeded services and software packages disabled or removed;
c. have unneeded accounts removed, default credentials changed, and anonymous access disabled;
d. be configured to deny network, shell, console and file system access unless specifically permitted;

e. have the latest security patches applied;
f. have media and network drive auto-play functions disabled;
g. restrict privileged actions to Privileged User accounts only;
h. forward security event logs to a central Security Information and Event Management (SIEM) solution, in accordance with the Logging, Monitoring and Alerting Procedure;
i. be configured with a personal firewall if operating on premises that are not owned or operated by the University;
j. be located in an appropriate network zone;
k. be located in a Demilitarised Zone (DMZ) if they require direct connection to external locations (inbound and outbound);
l. prohibit access to malicious or potentially dangerous websites;
m. enforce user access in accordance with the access control sections of this Policy;
n. be monitored by intrusion detection and/or prevention solutions that notify the IT Cyber Security team; and
o. have centrally managed real-time anti-malware software installed, in accordance with the Malware section in this Policy.

(54) IT Resources that handle Highly Sensitive information (refer Information Classification and Handling Procedure) must be built/configured in accordance with, but not limited to, the following requirements:

a. application whitelisting to restrict application and script execution to only those folders or directories required to perform the business function;
b. have USB ports, floppy disk drives and optical drives disabled;
c. be monitored by change detection software that monitors critical system files; and
d. log all data-level access to Highly Sensitive information to a central log server.

(55) Firewalls must be built/configured in accordance with, but not limited to, the following requirements:

a. firewalls must only allow the ports required for the business function and deny all other traffic;
b. firewalls protecting an IT Resource in a DMZ should not be configurable from the IT Resource they are protecting; and
c. non-production environments must be separated from production environments by a firewall solution.

(56) Firewall rule changes must be reviewed and approved by the Cyber Security team to determine if they meet one or more of the following conditions:

a. permits traffic to or from external (internet or Third-Party) locations;
b. permits traffic between production and non-production environments;
c. permits a large number of source or destination addresses (greater than 10);
d. permits all source or destination protocols (an “ANY” rule);
e. permits a broad range of source or destination protocols (greater than a range of 20 ports);
f. establishes a new network path to an external party;
g. uses protocols that pass credentials or data in clear text (SNMP, POP3, IMAP, LDAP, FTP, TFTP, Telnet, rexec, rlogin, rsh/.);
h. uses protocols that are known as an avenue for computer worms (SMB/CIFS TCP445 & TCP139, MS-RPC TCP135, RDP TCP3389 etc); and/or
i. facilitates remote control of computers (RDP TCP3389, VNC TCP5500 TCP5800 TCP5900, pcANYWHERE TCP5631 UDP5632 etc).

(57) Web application environments should adhere to the following requirements:

a. reside in at least a two-tier network architecture (application and database);
b. servers in the database zone should not be permitted to initiate connections directly with the application zone; and
c. servers directly involved in hosting internet-facing web applications should be blocked from initiating outbound connections.

(58) Access to specific IT Resources should adhere to the requirements outlined within the following table:

Type	**Requirements**
Database Access	non-production applications and databases must not contain production data; 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; applications that integrate with a database must be assigned a unique application account, used exclusively for the interactions with the database; and 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.
Root Access	root Access accounts should only be used in the case of an emergency; root Access account passwords should be stored in a secure digital format protected by strong encryption; root Access accounts should only be accessible by the minimum number of support staff required; and root Access account passwords should not be sent by email, instant message technology or over the phone.
Console Access	require re-authentication after 20 minutes of inactivity if facilitating access to Highly Sensitive information; and not be directly accessible from the internet with a single factor of authentication.
System-to-System Access	not be used by individuals for day-to-day operations; be either certificate based or consist of a password of at least 16 characters; can be set to never expire; and be protected by strong encryption or restrictive file system permissions when stored (only permit access to the required application accounts).
Remote Access	only be permitted via an approved Virtual Private Network (VPN) solution; be protected by strong encryption; and be removed immediately when no longer required.

(59) A message that discourages unauthorised access and notifies the user of activity monitoring should be displayed before a user attempts to logon to an IT Resource, as outlined in the table below:

IT Resource Type	**Warning Message**
Computers and Network Devices	Example: 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.
Application	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.

Section 4 - Guidelines

(60) Nil.

Section 5 - Definitions

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

a. Affiliates means contractors, agents, honorary, clinical or adjunct appointees and consultants of the University.
b. Confidentiality, Integrity, and Availability (CIA Triad) refers to the core principles of information security, ensuring that information is protected from unauthorised access (confidentiality), remains accurate (integrity), and is accessible when required (availability).
c. Information means any information in either physical or electronic format that is generated, created, stored, purchased or received during the conduct of University operations.
d. Information Technology Resources, or IT Resources, includes, but is not limited to:
    i. All computers and all associated data networks and systems, internet access and network bandwidth, email, hardware, data storage, computer accounts, all OneID systems, media, software (both proprietary and those developed by the University) and telephony services.
    ii. Information Technology services provided jointly, or as part of a joint venture between the University and a research centre, school, institute affiliated with the University, a subsidiary organisation owned by the University or any other partner organisation.
    iii. Information Technology services provided by Third-Parties that have been engaged by the University. Privileged User Account means an account with elevated permissions to manage and make system-wide changes (e.g., configure systems, install software, access sensitive data).
e. Standard User Account means an account used for day-to-day tasks with a restricted set of permissions.
f. Third-Party means an individual or organisation working under contract with the University.

Status and Details

Status	Current
Effective Date	23rd July 2026
Review Date	23rd July 2031
Approval Authority	Deputy Vice-Chancellor (People and Operations)
Approval Date	23rd July 2026
Expiry Date	Not Applicable
Responsible Executive	Eric Knight Deputy Vice-Chancellor (People and Operations)
Responsible Officer	Jonathan Covell Chief Information and Digital Officer
Enquiries Contact	Andrew Karvinen Chief Information Security Officer