Information Security Procedure

Section 1 - Purpose

(1) The purpose of this Procedure is to set rules for and explain:

a. Access Control;
b. Information Security Incident Management;
c. Information Security Requests ('Code Yellow'); and
d. Password Management Information Systems Acquisition, Development and Maintenance.

(2) This Procedure is closely aligned with the 2015 New South Wales Government Digital Information Security Policy Compliance with Minimum Controls Core Requirement as recommended for universities by the New South Wales Government ICT Strategy and draws from the following guidelines for the Information Security Industry standards:

a. AS/NZS ISO/IEC 27005:20011 Information technology — Security techniques — Information security risk management; and
b. AS ISO/IEC 27002:2015 Information technology — Security techniques — Code of practice for information security controls.

Scope

(3) This Procedure applies to:

a. the management of all matters relating to information security within the University;
b. all University information systems and information assets regardless of the media on which information is stored, the locations where the information is stored, the technology used to process the information, or the people and roles who handle the information;
c. all Information resources owned, leased, operated, or under the custodial care of third parties operated on behalf of the University; and
d. all individuals accessing, using, holding, or managing University Information resources on behalf of the University.

(4) Data that is personal to the User of a University IT Resource and is stored, processed, or transmitted on that IT Resource as a result of incidental personal use is not considered University data. However, University data stored on non-university IT facilities must be verifiably protected according to the minimum security standards outlined in the Information Security - Data Classification Procedure and Standards.

Section 2 - Policy

(5) Refer to the Cyber Security Policy.

Section 3 - Procedures

Part A - Access Control

Operational requirement for access control.

(6) Objective: To control access to information.

a. Access to information, information processing facilities, and operational processes must be approved on the basis of operational and security requirements by the nominated owner.
b. Anonymous access is not permitted to assets classified as sensitive.
c. Access control rules and rights for each user or group of users must be clearly stated.

User Access Management

(7) Objective: To ensure authorised user access and to prevent unauthorised access to information systems.

a. Formal procedures must be in place to control the allocation of access rights to information systems and services.
b. The procedures must cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.
c. Special attention must be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

User registration

(8) There must be a formal user registration and de-registration procedure (user registration form) in place for granting and revoking access to all information systems and services.

(9) The access control procedure for user registration and de-registration must include:

a. using unique user IDs to enable users to be linked to and held responsible for their actions. The use of group IDs (role-based accounts) must only be permitted where they are necessary for operational reasons, and must be approved and documented;
b. ensuring service providers do not provide access until authorisation procedures have been completed;
c. maintaining a formal record of all persons registered to use the service;
d. immediately removing or blocking access rights of users who have changed roles or jobs or left the University;
e. periodically checking for, and removing or blocking, redundant user IDs and accounts after inactivity for 90 days, deletion after 180 days; and
f. redundant user IDs are not to be issued to other users.

Privilege Management

(10) The allocation and use of privileges must be restricted and controlled.

(11) The principle of least privilege must be applied. Approved access by the asset owner must only be granted if it is deemed necessary to support a legitimate operational requirement.

(12) Privileges must be assigned to a different user ID from those used for normal operational activity.

(13) The University will monitor IT Resources and:

a. review privileged access quarterly, to ensure continued access is required;
b. log and audit use of and changes to IT systems and services; and
c. retain logs for monitoring and investigations.

(14) Staff authorised to undertake routine monitoring of IT Resources and extraordinary monitoring can only do so in accordance with University policies.

User Responsibilities Objective

(15) To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

a. A clear desk and clear screen policy must be implemented to reduce the risk of unauthorised access or damage to papers, media, and information processing facilities for information classified as sensitive.

Network Access Control

(16) Objective: To prevent unauthorised access to networked services.

a. Access to both internal and external networked services must be controlled.

Use of network services

(17) Users will only be provided with access to the services that they have been specifically authorised to use.

User authentication for external connections

(18) Appropriate authentication methods are required to control access for remote users.

Equipment identification in networks

(19) Automatic equipment identification must be considered as a means to authenticate connections from specific locations and equipment.

Remote diagnostic and configuration port protection

(20) Physical and logical access to diagnostic and configuration ports must be controlled.

Segregation in networks

(21) Groups of information services, users, and information systems must be segregated on networks.

Network connection control

(22) For shared networks, especially those extending across the University's boundaries, the capability of users to connect to the network must be restricted, in line with the access control policy and requirements of the business applications.

Part B - Information Security Incident Management

Reporting information security events and weaknesses

(23) Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

a. All employees, contractors and third party users must be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of University assets. They must report any information security events and weaknesses as quickly as possible.
b. Users must not publicise security incidents, as publicity increases risks to the University.

Reporting and management of information security events

(24) Any known or suspected information security event or weakness will be reported to the IT Service Desk immediately by calling +61--2 9850 HELP (4357), or by email to onehelp@mq.edu.au.

(25) Significant incidents are incidents that have implications on personal security, Occupational Health and Safety, breaches of privacy or incidents that may involve the administrative or academic manager.

(26) Significant incidents must be reported to the Chief Information Officer immediately.

(27) Faculties or Offices that cannot positively determine that the reported security event or weakness was a false positive will report the suspected information security event or weakness to the Chief Information Officer or the Chief Information Security Officer immediately.

(28) The ICT security team will evaluate the information and determine the appropriate course of action. Any investigation outside the approval of the ICT Security team will be managed by disciplinary processes as per the Acceptable Use of IT Resources Policy.

(29) A process of continual improvement will be applied to the response to, monitoring, evaluating, and overall management of information security incidents.

(30) Where evidence is required, it must be collected to ensure compliance with legal requirements.

(31) In accordance with Australian Guidelines for the Management of IT Evidence, HB171-2003, only defined security investigators are to collect security incident evidence. The Information Security Manager will ensure proper chain-of-custody of evidence when it is suspected that the information security event may result in legal action.

Part C - Information Security Requests ('Code Yellow')

(32) CodeYellow is a procedure and mechanism to ensure the best signal-to-noise ratio available when information security action is needed.

(33) CodeYellow is designed to enforce policy, create a viable audit trail, streamline approval and decrease the time taken to take action. It represents a concrete improvement on the current practice of unaccountable email trails, delays due to unavailability of decision makers.

(34) CodeYellow is not an emergency hotline suitable for physical or personal danger or safety alarms. CodeYellow depends on an external software service (OneHelp) which does not have uptime, real-time alerting, emergency broadcast or security characteristics suitable for these kinds of situations.

(35) CodeYellow works like this:

a. An incident occurs and is assessed by a reporting entity.
b. The reporter raises an incident by one of three methods:
    i. email: codeyellow@mq.edu.au;
    ii. OneHelp; or
    iii. telephone: +61-2-9850-HELP otherwise known as x4357.

c. Because different provisions apply, each CodeYellow must be classified as either:
    i. account access / lockout (where an account holder's access is to be terminated or an alternative account holder is granted proxy access);
    ii. account extension (where an account holder is approved by their Dean / Head of Office for access outside normal policy);
    iii. digital surveillance (where information gathering is required without the knowledge of an account holder);
    iv. privacy breach (where a suspected contravention of privacy policy has occurred and requires investigation); or
    v. law enforcement / regulatory (where a court, police or homeland security action has been requested or ordered).
d. The resulting OneHelp ticket is routed to the Macquarie IT management team to ensure visibility by senior personnel, bypassing normal level 1,2 and 3 support teams.
e. A OneHelp ticket approval process is initiated to key executives designated as having CodeYellow responsibility by reason of policy.
f. Email notification to this approval group is initiated and can be responded to directly in email by clicking "yes / no" which will update the OneHelp audit trail to record the decision. The ticket cannot be actioned without the correct approval.
g. Once the requisite combination of approvals is received, any starfleet member assign the ticket to the correct people to action it.

Approval Mechanism

(36) A OneHelp automated approval process is used as a prerequisite to actioning a CodeYellow. The key personnel involved are the current Chief Information Officer (CIO), Director, Human Resources (Dir, HR), General Counsel (GC) and Deputy Vice-Chancellor. Approval works like this (a composite view across policies):

Issue concerning	Staff	Students	Other Party	How many to approve	Associated Policy	Definition
Account access / lockout	CIO and Director, Human Resources	CIO and DVC	CIO and DVC	1	Acceptable Use of IT Resources Policy	1) Account Access: Person other than allocated owner needs access to email account after owner has left MQ. Access is only given to the email archive (Postini) and never the account directly. This is to keep the identity of account owner intact. System Administrator of Postini can grant access. 2) Lockout: MQ Employee is being locked out of their account for disciplinary reasons or has been dismissed etc. MAY NEED TO ACT IMMEDIATELY. Sys Admin's need to lock / block OneID account access.
Account extension	CIO or Director, Human Resources	CIO or DVC	CIO or DVC	1	Acceptable Use of IT Resources Policy	Academic or professional staff member requests access to their email after they leave MQ (for more than what is already allowed). The IT Service Desk can extend account after access is approved.
Digital surveillance	CIO and Director, Human Resources	CIO and DVC	CIO and GC	1	Acceptable Use of IT Resources Policy and Cyber Security Policy	SERIOUS and SENSITIVE. Governed by legislation. Approval will be given to conduct digital surveillance on email or digital records, disk copy of computer etc. CIO will coordinate.
Privacy breach	GC and CIO	GC and CIO	GC and CIO	1	Cyber Security Policy	Means that an MQ system has been hacked or breached. Staff need to act extremely quickly to mitigate breach. Coordination point may come from many places – IT Security to be made aware a.s.a.p.

Issue concerning	Staff	Students	Other Party	How many to approve	Associated Policy	Definition
Law enforcement / regulatory	GC or CIO	GC or CIO	GC or CIO	1	Agreement with Legal Counsel	Subpoena related searches. Subpoena from state or Federal police will be received by Legal Counsel who may ask that digital records be provided directly to them. NEVER DEAL WITH POLICE DIRECTLY, ALWAYS REFER THEM TO MQ Security. Nominated people within the IT Service Desk can provide information after approval given.
Personal Information Access	GC or CIO	*Pre Approved for Deidre Anderson Darren Peters Michael Carley John Durbridge	GC or CIO	Pre approved for student information. 1 for staff information.	Acceptable Use of IT Resources Policy and Privacy Policy	1) IT Service Desk can release student information to Deidre Anderson, Darren Peters, Michael Carley or John Durbridge immediately if they ask for it - its pre approved. 2) Approval is needed to release staff information by General Counsel or CIO. Nominated people within Macquarie IT / IT Service Desk can provide information after approval given.

(37) A member of the Senior Leadership Team can act as a proxy for the CIO in the event of unreachability and are part of the IT management team that the ticket is routed to.

(38) The Deputy Vice-Chancellor or Vice-Chancellor both have executive approval privilege should the situation warrant it or should one of the required approvers be unavailable - this is the only CodeYellow bypass mechanism. Invocation of this approval is also required to be noted on the ticket.

Limitations

(39) All designated people in the tech group receive CodeYellow notifications, regardless of the type of approval.

(40) Each type of request strictly requires the approvers nominated unless policy changes.

(41) OneHelp itself is not a security mechanism; it is a tasking mechanism that can be seen by technicians. The system is not designed to be the case management mechanism for the issue, just the approval and execution of IT tasks.

(42) Although regular support centre processes are short-circuited by CodeYellow to limit the number of eyes on the incident and reduce the escalation time, a technician with the URL for a CodeYellow could access the incident. This is, of course, by design and necessary for efficient task flow.

Part D - Password Selection and Management

(43) The following controls must be applied:

a. user-level passwords must be kept confidential. If your password has been compromised – change your password immediately;
b. user accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user;
c. passwords must not be inserted into email messages or other forms of electronic communication;
d. passwords must never be written down or stored online;
e. passwords must never be included in scripts;
f. initial passwords must be changed on first-time use;
g. procedures to verify the identity of the requesting a new, replacement or temporary password must be followed by the persons performing the change;
h. default vendor passwords must be altered following the installation of systems or software;
i. where possible, account must be disabled after five (5) unsuccessful login attempts for an account that access sensitive information;
j. where possible, the last nine (9) passwords must not be re-used;
k. maintain separate passwords from internal and external system access; and
l. a keyed hash must be used where available e.g. SNMP.

(44) All user-level and system-level strong passwords must conform to the following minimum of three (3) of the following criteria, where possible:

a. contain both upper and lower case characters (e.g., a-z, A-Z);
b. have digits and punctuation characters as well as letters e.g.,$%^&;
c. is at least eight characters long;
d. is not a word in any language, slang, dialect, jargon, etc;
e. is not based on personal information, names of family, etc; and
f. create a strong password that is easy to remember. Think of a phrase that you can easily remember e.g. "This May Be One Way To Remember" and the password could be: "TmB1w2R!".

Part E - Information Systems Acquisition, Development And Maintenance

Correct processing in applications

(45) Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications.

a. Input data validation
    i. Data input to applications must be validated to ensure that this data is correct and appropriate.
b. Message integrity
    i. Requirements for ensuring authenticity and protecting message integrity in applications must be identified, and appropriate controls identified and implemented where classified as sensitive.

Cryptographic controls

(46) Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

a. **Key management**

i. Key management must be in place to support the University's use of cryptographic techniques.
ii. All cryptographic keys must be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorised disclosure.
iii. Equipment used to generate, store and archive keys must be physically protected.
iv. A key management system must be based on an agreed set of standards, procedures, and secure methods for:
- generating keys for different cryptographic systems and different applications;
- generating and obtaining public key certificates;
- distributing keys to intended users, including how keys must be activated when received;
- storing keys, including how authorised users obtain access to keys;
- changing or updating keys including rules on when keys must be changed and how this will be done;
- dealing with compromised keys;
- revoking keys including how keys must be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves the University (in which case keys must also be archived);
- recovering keys that are lost or corrupted as part of operational continuity management, e.g. for recovery of encrypted information;
- archiving keys e.g. for information archived or backed up;
- destroying keys;
- logging and auditing of key management related activities; and
- proactive renewal of expired keys, prior to the expiration date.

Security of system files

(47) Objective: To ensure the security of system files.

a. Control of operational software:
i. There must be procedures in place to control the installation of software on operational systems.
b. Access control to program source code:
i. Access to program source code must be restricted.

Security in development and support processes

(48) Objective: To maintain the security of application system software and information.

a. Change control procedures
i. The implementation of changes must be controlled by the use of ICT change control procedures.
b. Technical review of applications after operating system changes
i. When operating systems are changed, critical applications must be reviewed and tested to ensure there is no adverse impact on University operations or security as part of ICT change control process.
c. Restrictions on changes to software packages

i. Modifications to software packages must be discouraged, limited to necessary changes, and all changes must be strictly controlled as part of the ICT change control process.

d. Outsourced software development
    i. Outsourced software development must be supervised and monitored by the University.

Technical vulnerability management

(49) Objective: To reduce risks resulting from exploitation of published technical vulnerabilities. Technical vulnerability management must be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

a. Control of technical vulnerabilities
    i. A centralised vulnerability management process must be established.
    ii. All information about technical vulnerabilities of information systems being used must be obtained from external authorities such as AUSCERT to a central point of control – Chief Information Security Officer.
    iii. Vendor ratings will be adopted.
    iv. The University's exposure to such vulnerabilities will be evaluated.
    v. An agreed timeline must be defined to react to notifications of potentially relevant technical vulnerabilities.
    vi. The appropriate measures in conjunction with the asset owner must be taken to address the associated risk.
    vii. A patch management process must be established, implemented and monitored for all systems, maintaining a minimum patch level of n-1. This process will be managed by the ICT change management policy.

Compliance

(50) Macquarie IT will monitor compliance with the Cyber Security Policy and related procedures. Users must promptly report breaches of the Cyber Security Policy and this Procedure and suspected information security weaknesses to the Chief Information Officer.

(51) Any breach of the Cyber Security Policy and related procedures may infringe relevant legislation as listed at the outset of this Procedure and expose persons to liability under such legislation.

(52) If any of the minimum standards contained within this document cannot be met on systems manipulating Confidential or Controlled data, an Exception Process must be initiated that includes reporting the non-compliance to the Chief Information Officer, along with a proposed risk assessment and management plan. Non-compliance with these standards may result in revocation of system or network access, notification of supervisors and reporting to the Office of Internal Audit.

(53) Any breach of this Cyber Security Policy or related procedures may result in formal disciplinary action for students in accordance with the Student Code of Conduct. Formal disciplinary action for staff will occur in accordance with the Misconduct / Serious Misconduct clauses as outlined in the Staff Code of Conduct, the Macquarie University Academic Staff Enterprise Agreement 2018 and the Macquarie University Professional Staff Enterprise Agreement 2018.

(54) Macquarie University may refer serious matters or repeated breaches to the Vice-President, People and Services, Director, Human Resources, the Head of the relevant Organisational Unit or to the appropriate external authorities which may result in civil or criminal proceedings.

(55) External providers who breach the Cyber Security Policy or related procedures will be subject to suspension of

access, termination of contract and / or further legal action.

Section 4 - Guidelines

(56) Nil.

Section 5 - Definitions

(57) Commonly defined terms are located in the University Glossary. The following definitions apply for the purpose of this Procedure. In this Procedure, unless a contrary intention appears:

a. 'Authority' means –
    i. in relation to the IT Resources generally, the Chief Information Officer or the Chief Information Officer's delegate;
    ii. in relation to a local facility, the relevant Head of Department, Executive Dean, or Deputy Vice-Chancellor, or a person nominated by the relevant Head of Department, Executive Dean, or Deputy Vice-Chancellor;
b. 'authorised purposes' means purposes associated with work or study in the University, provision of services to or by the University, which are approved or authorised by the relevant officer or employee of the University in accordance with University policies and procedures or pursuant to applicable contractual obligations, limited personal use, or any other purpose authorised by the relevant Authority;
c. 'Chief Information Officer' means the person holding or acting in that position in the University, or any other person nominated by the Vice-Chancellor to exercise that role for the purpose of this Procedure.
d. 'Confidential Data' means one of three data classifications defined within the Information Security - Data Classification Procedure and Standards. Data that is subject to restrictive regulatory obligations in relation to the access, distribution, retention and / or destruction.
e. 'Controlled Data' means one of three (3) data classifications defined within the Information Security - Data Classification Procedure and Standards. Data that is not generally created for or made available for public consumption, but that is subject to release to the public through a request via the Government Information (Public Access) Act 2009 or other applicable Commonwealth or State Law.
f. 'Data' means elemental units, regardless of form or media, that are combined to create information used to support research, teaching, and other University business processes. Data may include but are not limited to: written, electronic video, and audio records, photographs etc.
g. 'Data Centre' means a facility used to house computer systems and associated components, such as telecommunications and storage systems.
h. 'Digital Data' means the subset of Data (as defined above) that is transmitted by, maintained, or made available in electronic media.
i. Director, Human Resources means the person holding or acting in that position in the University, or any other person nominated by the Vice-Chancellor to exercise that role for the purpose of this Procedure;
j. 'illegal material' means material the creation, transmission, storage, downloading or possession of which contravenes or if done in New South Wales would contravene the criminal law as it applies in any jurisdiction in Australia;
k. 'Information Security' is the protection of information and supporting systems from a wide range of threats in order to ensure business continuity, minimise operational risk, and maximise return on investments and operational opportunities.
l. 'Information Security Management System (ISMS)' the policies, procedures, standards, plans, metrics, reports,

resources, and services adopted for the purpose of systematically securing University Information Resources by applying a risk-based management process

m. ‘Macquarie IT’ means the Macquarie University IT Department.

n. ‘intellectual property’ includes the rights relating to –
    i. literary (including computer programs), artistic, musical and scientific works;
    ii. multimedia subject matter;
    iii. performances of performing artists, phonograms and broadcasts;
    iv. inventions in all fields of human endeavour;
    v. scientific discoveries;
    vi. industrial designs;
    vii. trademarks, service marks and commercial names and designations;
    viii. plant varieties;
    ix. circuit layouts; and
    x. confidential information.

o. ‘limited personal use’ means use that –
    i. is of a purely personal nature and not for financial gain;
    ii. does not directly or indirectly impose an unreasonable burden on any IT Resources;
    iii. does not unreasonably deny any other user access to any facilities;
    iv. does not contravene any law in any jurisdiction in Australia or any University statute, regulation, policy or procedure; and
    v. in the case of staff, does not interfere with the execution of duties.

p. ‘misuse’ has the meaning set out in the Acceptable Use of IT Resources Policy Acceptable Use of IT Resources - Misuse Schedule;

q. ‘staff’ means staff of the University;

r. ‘student’ includes a person who was a student at the time of any alleged breach of this Procedure, and a person who is a student for the purposes of the Student Discipline Rules and Student Discipline Procedure;

s. ‘University copyright officer’ means the officer designated by the Vice-Chancellor as responsible for overseeing copyright issues within the University;

Status and Details

Status	Historic
Effective Date	22nd February 2021
Review Date	8th March 2021
Approval Authority	Vice-President, People and Services
Approval Date	21st June 2016
Expiry Date	28th April 2021
Responsible Executive	Nicole Gower Vice-President, Professional Services
Responsible Officer	Tim Hume Chief Information Officer +61 2 9850 1660
Enquiries Contact	Andrew Wan Chief Information Security Officer Information Technology