

OVERVIEW

The Vice-Chancellor of Macquarie University is responsible for:

- protecting the confidentiality, integrity and availability of information in the custody of the University and the software and hardware that processes it;
- the related privacy rights of the University's students, faculty and staff and other individuals.
- compliance with relevant Commonwealth and State legislation and regulations, such as intellectual property and copyright;
- the preservation of information in the event of a disaster; and
- respecting the rights of other users of the Internet and their similar needs to protect information and computer systems.

Compliance with this policy and all supporting standards and procedures is mandatory for staff, students, contractors, and other third parties who in the course of their work or studies have access to the University's information, information systems and other facilities on the computer network. The unauthorised modification, deletion, or disclosure of information included in Macquarie University information systems can compromise the integrity of university programs, violate individual privacy rights and possibly constitute a criminal act, and is expressly forbidden.

This policy is not limited to those systems and equipment operated and maintained by the central Information Systems Department but applies to all information systems and computer equipment on campus or belonging to the university.

DEFINITIONS

For the purposes of this policy:

- **Confidentiality** means restricting access to information to authorised persons at authorised times and in an authorised manner;
- **Integrity** means safeguarding the accuracy and completeness of information; and
- **Availability** means ensuring that authorised users have access to information at authorised times.
- **Information Asset** means any intangible electronic information (separate from the media upon which it resides) owned, controlled or hosted by Macquarie University
- **Information System** means any tangible item such as hardware, software, communications facilities and networks, used to store, process and transmit Information Assets owned, controlled, or hosted by Macquarie University.

SECURITY POLICY

The Macquarie University policy is:

1. Information security governance framework

The Macquarie University ICT Policy Committee has delegated responsibility and authority for all matters related to information security including:

- a. Monitoring the ongoing relevance of the Information Security policy, and implementing and disseminating revisions as necessary;
- b. Considering and ruling on requests for exemption from the Information Security policy;
- c. Monitoring compliance with the Information Security policy; and
- d. Actioning Information Security policy violations.

2. Asset classification and control

- a. All Information Systems and Information Assets must be uniquely identified, assigned a classification and an Information Owner; and
- b. The Information Owner will decide who is authorised to access an Information System or Information Asset, the type of access (read, modify, delete, copy), where it can be accessed, when it can be accessed, and if and how it may be made public.

3. Personnel security

- a. Every individual who uses or has access to the University's information, information systems or computer equipment be made aware of the 'Macquarie University Information Security Policy'; and
- b. They be advised that they are responsible for maintaining information security, including, but not limited to:
 - I. Complying with all information security policies, standards and procedures;
 - II. Ensuring information is only used for the purpose it was collected as defined by the Information Owner;
 - III. Maintaining confidentiality of passwords; and
 - IV. Promptly reporting evidence of attempts to compromise security or misuse of information or information systems to the Information Owner

4. Physical and environmental security

All Information Systems or Information Assets classified as "critical" must be housed in a physically secure area, protected by a defined security perimeter, with appropriate security barriers and entry controls. It must be physically protected from unauthorised access, damage and interference.

5. Communications and operations management

- a. Communications of sensitive Information Assets, either within Macquarie University facilities or involving third parties, must be secured in a proper manner commensurate with the value and sensitivity of the Information Assets; and

- b. Appropriate processes be implemented and maintained in the general University operation to ensure that Information Systems and Information Assets are protected from electronic attacks, threats and vulnerabilities.

6. Access control

- a. Access to Information Assets and Information Systems will be granted in a controlled manner, by the Information Owner, driven by business requirements such as the user's role or the "need to know" principle; and
- b. Read only access to Information Assets classified as public does not require a formal authentication and authorisation process.

7. Systems development and maintenance

Appropriate security is to be designed and implemented into all stages of the Information System Life Cycle (design, implementation, operation, and disposal).

8. Business continuity management

- a. All Critical Information Systems have a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to ensure the ability to recovery from failure or unexpected interruption; and
- b. The Information Owner is responsible for the implementation of a routine of risk assessment in order to refine the recovery requirements. The Business Continuity and Disaster Recovery Plans must be updated to reflect these refinements.

9. Compliance

- a. All applicable legal, statutory, contractual or regulatory requirements for information security will be documented and defined by the University's solicitor; and
- b. Every individual who uses or has access to information, information systems or computer equipment will be made aware of their responsibilities to comply with all legal, statutory, contractual or regulatory requirements pertaining to the information or information systems.

Approved by the Macquarie University ICT Policy Committee
9 August 2004