

## **Staff Guide to the Information Security Policy**

This information will guide you as a staff member in understanding your responsibilities to help ensure the integrity, availability and confidentiality of Macquarie University's information assets. If you are responsible for information assets which are owned, controlled or hosted by Macquarie University, refer to the [Information Owner and Information Custodian Guide](#).

### **Overview of Information Security Policy**

Macquarie University has created a new Information Security Policy through a consultative process within the university community to provide the foundation of new security controls.

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. This includes for example, eReserve, eLearning, Digital Records of Lectures, etc.
- **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

## Information Security Policy Contents

Macquarie University Information Security Policy consists of nine sections. Use the hyperlinks to access the relevant sections of the detailed Information Security Policy:

### 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;
- a Considering and ruling on requests for exemption from the Information Security policy;
- b Monitoring compliance with the Information Security policy; and
- c Actioning Information Security policy violations.

As a staff member, your access to and use of information assets may be [logged](#) to ensure that if required in the event of an incident, an approved investigation can be carried out to ensure that you have continued to act in compliance to this Information Security Policy. You will also be required to make yourself familiar with any updates to this Policy when you are notified of an update.

## **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.

As a staff member you will be provided with access to information as determined by the information owner. For example you may be given access to student grades. The use of the student grade information will need to be in compliance with the asset classification. Based on the information classification, you will not be able to copy the grades, send them to any third parties and would need to comply with the Information Owner's procedures when sharing this information with students.

## **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

As a staff member, your responsibilities regarding security will be documented by the Information Owner. You should ensure you are familiar with your responsibilities.

When using information you will need to be aware of the restrictions of use of the information asset. For example, when using eReserve, it is a classified asset and some restrictions will apply. In general, the use of classified information is similar to using a book. There are Copyright laws which prevent you from copying the information and there may also be rules about how you can disseminate and store the information.

Personal details including address and phone numbers are forms of classified information, and there will be rules about where the information can be stored, how it can be disseminated and to whom it may be disseminated. These Copyright laws also apply to downloading, copying and disseminating movies.

Here are a few simple rules to follow to keep your [password](#) confidential and to protect your ID file:

- Create strong passwords not using family members' names, favourite teams or activities or any dictionary words.
- Change your password regularly and do not share your new one with anyone
- Guard against others who may peer over your shoulder while you're keying in your password in open areas, i.e. the library
- Before leaving the workstation you are working at, prevent a passer-by from browsing through your messages or composing messages that appear to have been sent by you by locking the workstation or logging off the system.

You are required to report to the Information Owner if you see evidence of attempts to compromise security or misuse information or information systems. If you're uncertain who the Information Owner is, contact the [IT Help Desk](#).

#### **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.

As a staff member, you may have access to critical information for example, student grades and personnel files; however the University will be responsible for physically protecting this information in soft copy format. If however, you carry out research by conducting a survey, this information may be classified as critical, in which case you will be required to protect this information by storing the research and survey results in a secure environment as defined by this Policy.

You will also be required to ensure that all information kept on your hard drive is backed up and you will need to ensure that these backups work. If critical information which is stored on your hard drive is lost, Macquarie University is impacted as productivity and critical information is lost.

For further assistance you can contact the [IT Help Desk](#).

## 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.

A virus is a program that is able to reproduce itself. Just like a biological virus, its effects can range from being mildly annoying to paralysing an entire system. Since many viruses remain hidden, you may not realise until it's too late that you have the potential to infect other PCs around the University. You will need to perform a virus scan on any floppy disks when using University PCs or on any [files downloaded from the Internet or from email attachments](#). The University's anti-virus software must not be removed, reconfigured, tampered with or stopped in a manner that would lessen the protection offered by the software. You may not retrieve information that might be considered offensive and you must avoid accessing Internet sites where such information is known to be published.

Staff may also not be in the possession of or develop viruses or other malicious software, unless this is approved work which is being carried out. If you require approval, please contact the [Information Security Officer](#).

If a staff member is required to [move hard copy information](#) around, the classification of this information must be determined to ensure that appropriate physical controls are put in place in line with this Policy. For example staff or salary information must be shredded and not thrown in a dustbin.

With the informal nature of the Internet, it is easy to assume that our Internet communications are private and our actions could never reflect negatively on Macquarie University. That's not true, however. Every [email message](#) sent out through an Internet gateway identifies our University as its source. Maintaining our reputation as an educational institution is critical to maintaining our high standards, and actions that dilute that image have very real costs to the University.

Existence of email messages will be logged, and the content stored if the email is saved and may be audited and reviewed during discovery acts if required through an approved process. When using email users must comply with policies regarding appropriate language as detailed on <http://www.ois.mq.edu.au/policy/mgrules.html>. Users who create messages containing inappropriate language may be subject to disciplinary action.

Sensitive information, for example personal information, salary information, staff performance information, etc. should only be generated in hard copy if necessary to complete business operations. Hard copy information which is classified as sensitive should also be stored in locked drawers, cabinets and specifically designated rooms, restricting access to only authorised staff.

Illegally or without authorisation accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's or organisations' systems (often known as "hacking") is not allowed. You may also not undertake any activity that might be used as a precursor to an attempted system penetration (i.e. port scan, stealth scan, or other information gathering activity).

## 6 Access control

- c 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
- a Read only access to Information Assets classified as public does not require a formal authentication and authorisation process.

If you require access to information which is protected within Macquarie University or information on the web which is protected or blocked you will need to contact the Information Owner. If you're uncertain who the Information Owner is, contact the [IT Help Desk](#).

Before storing University information on publicly available sites, for example audio recorded files of lectures, Information Owner approval must be obtained.

When working remotely a greater security exposure exists. Therefore all the Security Policies continue to apply to staff members working from home or from other remote sites. Authorisation will need to be obtained from Information Owners to work remotely using University information. If you're uncertain who the Information Owner is, contact the [IT Help Desk](#).

Before storing University Information Assets which are private, confidential or secret, on mobile devices, e.g. laptops, palmtops, USB device, etc. the Information Owner must also be consulted to ensure that appropriate physical access controls are applied.

## **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).

If you are responsible for developing Information Systems, the security requirements must be determined prior to the application development phase as detailed in [this section](#) of the Policy. The development of Information Systems includes systems like the scheduling system which is an excel spreadsheet and access databases.

## **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.

As a staff member you will not be required to develop any Business Continuity Plans or Disaster Recovery Plans, unless you are an Information Owner. If you are an Information Owner, refer to this section in the [Manager's Guide](#) for further information.

## **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,

This Guide forms the basis for providing you with an awareness of your responsibilities with regards to information security.

You will need to comply with various [legal requirements](#) including intellectual property rights, safeguarding of organisational records and data protection and privacy of personal information.

It is unethical to make a copy of software and give it to a friend or use it for personal reasons. All University staff and students are prohibited from loading any illegal software on any of the University's computer resources or personal devices attached to the University's network. If you need to use shareware or freeware, you will need the approval of the division or head of office to load this software on University computer resources.