

Student Guide to the Information Security Policy

This information will guide you as a potential or current student at The College of Law, in understanding your responsibilities to help ensure the integrity, availability and confidentiality of The College of Law's information assets

1. Overview of Information Security Policy

College of Law has created an Information Security Policy through a consultative process within the College community to provide the foundation of new security controls

The Director Information, Systems and Technology of The College of Law is responsible for:

- Protecting the confidentiality, integrity and availability of information in the custody of the College and the software and hardware that processes it
- The related privacy rights of the College's students, faculty, 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 College's information, information systems and other facilities on the computer network. The unauthorised modification, deletion or disclosure of information included in College of Law information systems can compromise the integrity of College 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 Technology department but applies to all information systems and computer equipment on College campuses or belonging to the College

2. Definitions

For the purposes of this policy:

- Information Confidentiality (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
- Availability – means ensuring that authorised users have access to information at authorised times
- Information Asset (Asset) – means any intangible electronic information (separate from the media upon which it resides) owned, controlled or hosted by The College of Law. This includes for example LPortal, student portal, iForums etc

- Information Technology (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 the College of Law

3. Information Security Policy Contents

The College of Law Information Security Policy consists of eleven sections. Use the hyperlinks to access the relevant sections of the detailed Information Security Policy

3.1. Information Security Policy Introduction

Integral to the efficient functioning of the College of Law is the requirement to secure its information assets. Securing information assets requires that the asset confidentiality, integrity and availability be assured in accordance with COLLAW's business requirements. It is the responsibility of COLLAW staff, students and individuals to protect all information (and information assets) encountered in the conduct of their duties.

The objective of the information security policy is to formally document and communicate to all parties a framework to manage the protection of information. This policy is available to all COLLAW employees and students and third parties on request.

This policy aims to ensure that the overall risk to COLLAW is maintained at or below an acceptable risk based on sound risk management strategies. An essential component of this process is that all persons interacting with information systems have an understanding of their rights and responsibilities with regard to security safeguards

Being enrolled as a student means you will be given access to some of the Information Assets of the College. This access is given on the condition that you will become familiar with the COLLAW Information Security Policy and abide by its provisions. This document is your guide to the main elements of the main Policy that affect students the most

3.2. Information Security Policy

The objective of the Information Security Policy is to ensure that all risks to the College of Law (COLLAW) information environment are identified and pro-actively managed. The Information Security Policy identifies and defines the roles and responsibilities.

The Security Policy document must encompass the following:

- All security relevant components of the COLLAW environment: and
- Roles and responsibilities of all security personnel associated with the COLLAW environment

Policy requirements also include:

- Regular review and maintenance of the policy and supporting documents
- Management endorsement

- Distribution to all individuals with access to COLLAW information services: and
- A set of supporting documents to assist in the implementation of the Policy (e.g. COLLAW security plans, operational procedures, standards and guidelines)

As a student your access to and use of information assets may be monitored to ensure that you continue 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

3.3. Personnel Security

The objectives of the Personnel Security policies are to minimise the effects of human error, theft and system misuse on the security of the COLLAW environment.

Personnel security is one of the most important elements in the overall security of COLLAW. Key elements of the Personnel Security policies pertaining to students are:

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

When using information you will need to be aware of the restrictions in use of the information asset. For example, when using the Learning Portal, 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. These copyright laws also apply to downloading, copying and disseminating movies.

3.4. Asset classification and Control

Asset Classification and Control ensures that all COLLAW information assets have been identified and classified so that mechanisms can be put in place to effectively monitor and control their use. In particular:

- All COLLAW assets must be accounted for and have an information owner who is ultimately responsible for the control of that asset. Enforcing accountability for assets ensures that appropriate protection can be maintained
- The information owner will decide who is authorised to access an Information System or Information Asset, the type of access, where it can be accessed, and if and how it may be made public

As a student you will be provided with access to information as determined by the Information Owner. For example you will be given access to soft copies of course notes via the Learning Portal. The use of these notes will need to be compliance with the asset classification. Based on the course notes classification, you will not be able to copy the notes and send them to a friend.

3.5. Physical and Environmental Security

The objective of physical and environmental security policies are to ensure that the confidentiality, integrity and availability of the COLLAW information assets are maintained.

Individual COLLAW users are responsible for the security of COLLAW information under their control. All Information Systems or Assets classified as “X-in-Confidence” 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 student you will have access to X-in-confidence material such as your grades. The College will be responsible for physically securing this information as stored on its Information Systems in electronic format

3.6. Communications and Operations Management

The objective of communications and operations management security is to ensure that the confidentiality, integrity and availability of COLLAW’s information assets are maintained through good operational management practices. This covers a diverse set of areas encompassing:

- applications management - Internet access, email, online services and content filtering
- network layer protection – network and communications security
- systems protection – authorised software and anti virus protection
- operational issues – operations management, remote equipment management and media management

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 too late that you have the potential to infect other information hardware assets (PC’s,

laptops etc) around the College. Virus scans must be performed on all removable media when using College workstations and on any files downloaded from the Internet or from email attachments.

All devices attaching to the College network (such as student laptops via the wireless network) must have current up-to-date anti malware software configured to scan all files as they are opened and/or transferred to and from the system

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 the College of Law. That's not true however. For example, Every email message sent out through an Internet gateway identifies our College as its source. Maintaining our reputation as an educational institution is critical to maintaining our high standards. Actions that dilute that image have very real costs to the College

Specific unacceptable uses of the Internet include:

- Any use which violates any Commonwealth or State law in Australia
- Any use for profit making activities, unless specific to COLLAW business activities
- Any use to intentionally seek information on, obtain copies of, or modify files or data belonging to others without authorisation of the file owner. Seeking passwords of others or the exchange of passwords is specifically prohibited
- Use for access to and distribution of illegal, indecent or obscene material, or pornography or the illegal duplication of copyright protected information; and
- Any use to intentionally develop or use any program designed to harass or harm other users or to infiltrate a computer or computing system and/or damage or alter the data or software components

Email messages are considered to be College records and may be monitored, audited and reviewed during discovery acts if required. When using email users must comply with the policies regarding appropriate language as detailed in the College's Quality Management System. Users who create messages containing inappropriate language may be subject to disciplinary action

3.7. Access Control

The objective of Access Control policies is to ensure that the confidentiality, integrity and availability of COLLAW's data cannot be readily compromised through inadequate logical access controls. Protection of data through access control ensures that only authorised individuals are able to receive and view sensitive customer and COLLAW information. In general:

- Access to COLLAW information systems, data and business processes will be controlled based on business and security requirements. Applying the need-to-know principle ensures that COLLAW information is kept confidential and assists in maintaining integrity
- Network segregation and sensitive systems isolation limits the connectivity between different parts of the COLLAW environment to prevent unauthorised access.
- Password management ensures that individual logons are effective for protecting systems (and their information) and maintains accountability for individual user actions.
- Mobile computing policies help to reduce the risk of disclosure of COLLAW information stored on mobile devices and help prevent the introduction of security threats

If you require access to information which is protected within the College of Law or information on the web which is protected or blocked you will need to contact the Information Owner. If you are uncertain who the Information Owner is contact the Service Desk

Here are a few simple rules to follow to keep your password confidential and to protect your user ID:

- Create strong passwords not using family members' names, favourite teams or activities or any dictionary word
- 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
- 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

Mobile devices (PDA's, smart phones, iPods, laptops, notebooks etc) are not permitted to connect to the COLLAW network unless approved by the IT Manager

Mobile devices will not be approved for connection unless recognised anti-

virus/anti-malware software is installed and running and the device has current signatures and system security patches.

3.8. System Development and Maintenance

The objective of system development and maintenance policies is to ensure that security is designed and implemented, from conception to production delivery and ongoing maintenance, into all aspects of COLLAW systems

It is unlikely that College of Law students will be directly affected by this aspect of the Information Security Policy

3.9. Business Continuity Management

Business continuity measures ensure that COLLAW assets and operations are protected against both major and minor disruptions that could lead to financial loss or serious detriment to the business. In general:

- Business Continuity Planning (BCP) needs to occur to ensure that the College of Law continues to operate in the presence of risks that could degrade the performance or availability of systems, or limit the accessibility of key resources and assets
- The BCP must include Disaster Recovery Planning (DRP) that indicates how COLLAW will respond to failure events, such as system failures or environmental misfortunes that result in interruptions to or destruction of critical systems.
- Capacity and availability planning, backups and redundancy that are built into the architecture of the IT environment ensure that information availability and integrity is high.

Well designed and comprehensively tested enterprise-wide business continuity and disaster recovery plans are essential to ensuring that COLLAW is well prepared for disruptions of any magnitude. These plans ensure that COLLAW can resume normal operations as soon as possible after an interruption

This section is not directly applicable to students

3.10. Compliance

The objective of compliance is to confirm that all necessary security measures have been implemented within the COLLAW environment allowing COLLAW to operate securely.

The defined and accepted Information Security Policy will comply with existing international, national and industry standards. Therefore organisational compliance with the Information Security Policy will facilitate accreditation of the COLLAW information environment

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