Purpose

The purpose of this document is to ensure that appropriate measures are put in place to protect corporate information and the Information Technology Services (ITS) systems, services and equipment of the Federation University Australia and associated infrastructure.

The objectives of the Information Security Policy are:

- To secure the University’s assets against theft, fraud, malicious or accidental damage, breach of privacy or confidentiality; and
- To protect the University from damage or liability arising from the use of its ITS facilities for purposes contrary to the Federation University Australia Legislation and Policies.

Scope

This policy applies to all University staff, students, Ballarat Technology Park, Associate or Partner Provider staff, or any other persons otherwise affiliated but not employed by the University, who may utilise FedUni ITS infrastructure and/or access FedUni applications with respect to the security and privacy of information.

Definitions
<table>
<thead>
<tr>
<th><strong>Application:</strong></th>
<th>A software package to perform a specific task (e.g., MS Word).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup:</strong></td>
<td>A means of making a duplicate copy of a system and/or data for the purpose of being able to restore a system should a failure or corruption occur.</td>
</tr>
<tr>
<td><strong>Bluetooth:</strong></td>
<td>A short range (10 meters) personal wireless connection of compliant devices.</td>
</tr>
<tr>
<td><strong>Computer Work Area:</strong></td>
<td>Is an area or office in which access to computer resources is made available.</td>
</tr>
<tr>
<td><strong>DRP:</strong></td>
<td>Disaster Recovery Plan.</td>
</tr>
<tr>
<td><strong>Incident:</strong></td>
<td>An occurrence of suspect or illegal activity.</td>
</tr>
<tr>
<td><strong>Infrastructure:</strong></td>
<td>All components that make up the computing facilities of the University.</td>
</tr>
<tr>
<td><strong>ITS:</strong></td>
<td>Information Technology Services.</td>
</tr>
<tr>
<td><strong>LAN:</strong></td>
<td>Local Area Network.</td>
</tr>
<tr>
<td><strong>NAL:</strong></td>
<td>Novell Application Launcher.</td>
</tr>
<tr>
<td><strong>Patch:</strong></td>
<td>Software updates intended to remove or reduce risks from known vulnerabilities.</td>
</tr>
<tr>
<td><strong>PC:</strong></td>
<td>Personal Computer.</td>
</tr>
<tr>
<td><strong>Portable Device:</strong></td>
<td>Any handheld, or smaller, device used to access University systems or resources such as, but not limited to, iPhone, Smart phones, PDAs, iPad, mobile phones, laptop or notebook computers and the like.</td>
</tr>
<tr>
<td><strong>SOE:</strong></td>
<td>Standard Operating Environment</td>
</tr>
<tr>
<td><strong>FEDUNI:</strong></td>
<td>Federation University Australia.</td>
</tr>
<tr>
<td><strong>Users:</strong></td>
<td>Those who utilise the computing facilities of the University.</td>
</tr>
<tr>
<td><strong>User ID:</strong></td>
<td>Login details assigned to a user to enable them to use the ICT facilities.</td>
</tr>
<tr>
<td><strong>Virus:</strong></td>
<td>A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.</td>
</tr>
<tr>
<td><strong>VOIP:</strong></td>
<td>Voice Over IP is a means of using the ITS network for transmission of voice phone calls.</td>
</tr>
<tr>
<td><strong>VPN:</strong></td>
<td>Virtual Private Network.</td>
</tr>
<tr>
<td><strong>WAN:</strong></td>
<td>Wide Area Network.</td>
</tr>
<tr>
<td><strong>Wireless:</strong></td>
<td>Computer devices that connect using radio signals rather than cables.</td>
</tr>
</tbody>
</table>

**Policy Statement**

The Information Security Policy determines how the ITS services and infrastructure should be used in accordance with ITS industry standards and to comply with strict audit requirements.


This Policy includes:

**Staff and Student Security**

**Acceptable Usage**
Logical Security
Data Security
Physical Security
Mobile / Portable and Hand Held Devices
Security Incident Management
Business Continuity
Breaches / Infringements

Staff and Student Security

Specify what is expected from staff, both permanent and contracted, and students alike as information security is the responsibility of all who utilise the information technology services.

Staff and Student Access

The University provides students and staff with access to computing and communications services in support of its teaching, learning, research and administrative activities. These facilities include access to email, Internet, file and print services, an integrated data network across all campuses, Service Desk and Student computer laboratories located across all campuses.

Users are responsible for maintaining the use and security of their assigned User IDs and all activity associated with that ID. Knowingly disclosing passwords to others will be deemed a breach of policy and could be referred to disciplinary procedures.

The University expects its staff, students and associates to take all reasonable steps to ensure the integrity and security of FedUni ITS systems and data.

Human Resources Responsibilities

It is the responsibility of Human Resources to ensure correct termination dates are entered into the HR system for staff terminations. After a fixed number of days from the date of termination, the staff account will be disabled. Following a further pre-determined number of days, the account will be deleted.

There are however, situations where an account may need to be disabled immediately and this can only be performed with the authorisation from the Executive Director, Information Technology and Business Solutions or delegated officer.

Contract / Temporary Access

Where temporary access is required for a specific purpose such as, but not restricted to, contract workers and ‘test’ accounts, a user expiry date based on the completion date of the required tasks must be used to ensure the temporary account is not accessible after that date.

In the case of ongoing maintenance and support from 3rd party companies, access must only be granted to the relevant facilities within the system and be restricted to only the systems for which they provide support.
Reliance on People

All specialised computing staff are required to ensure that all systems and procedures are well documented and that there are others who can act in a backup capacity as required.

Managers Supervisors and Heads Responsibilities

It is the responsibility of managers, supervisors, School and Section Heads to be familiar with Information Security Policies and their requirements.

Acceptable Usage

Identification of what is deemed acceptable (or unacceptable) usage of network, communication and Internet services.

Network Usage

The University provides students and staff with access to computing and communications services in support of its teaching, learning, research and administrative activities.

By signing the appropriate forms for obtaining access to the University computing facilities, or accepting the online compliance button, users agree to abide by all policies that relate specifically to the use of these facilities. Any breach of these policies will be deemed an infringement and dealt with accordingly which could result in suspension of access privileges or in severe cases, legal authorities will be involved.

Interfering, in any way, with the University network or associated equipment, be it intentional or accidental, is not permitted. Any such interference will be acted upon and may result in removal from the University network until an investigation can be completed and the source of the interference is removed.

Electronic Communications

Federation University Australia encourages staff and students to appropriately use electronic communication in order to achieve the mission and goals of the University. The University encourages the use of electronic communication to share information, to improve communication and to exchange ideas. Given that universities place high value on open communication of ideas, including those new and controversial, the intention of the University is to maximise freedom of communication for purposes that further the goals of the University.

The electronic communications services must not be used for the distribution of material that may be deemed offensive, discriminatory or defamatory or the publishing or advertising of personal events or activities.

All usage must comply with the Use of Computing and Communication Facilities Policy.

Internet Usage

The University encourages staff and students to use the internet in order to further the strategic and operational objectives of the University. The University encourages the use of the Internet to share information, to improve communication and to exchange ideas.

Inappropriate usage of Internet facilities includes, but is not restricted to, accessing or posting of discriminatory, defamatory, offensive material or material that may create or promulgate a negative impression of the University.
Any staff or student required, as part of their job function or course of study, to access information on the Internet that may be deemed inappropriate, must obtain written authorisation from the Dean or Director with a copy submitted to the Information Security Officer.

All usage must comply with the Use of Computing and Communication Facilities Policy.

Internet Content Filtering

The University employs Internet Content Filtering technology as a tool in meeting its duty of care obligations by preventing students under the age of 18 from being exposed to inappropriate material including, but not limited to, adult content when utilising University provided internet access.

Mobile Devices

Mobile devices including, but not limited to, laptop and netbook computers, mobile phones, smart phones and tablet devices, are all subject to the same policies and procedures as for other computing and communication devices.

Refer to the Use of Computing and Communications Facilities Policy.

In addition, University supplied mobile devices must be configured with a password or pin code in order to access the device. Preferably, a password or phrase should be used, but at a minimum, a four (4) digit PIN code is acceptable. This becomes essential if corporate data and/or email is held or accessed from the device.

Logical Security

Implementing a suitable environment that protects the integrity, availability and confidentiality of FedUni data by using logical or ‘computerised’ controls and processes.

Software Security

Software security specifically relates to access rights and protection of software packages supplied by, and for the use by, FedUni computer services infrastructure. All users of the network are supplied with a User Account for authentication and allocation of appropriate access rights to network facilities including software. Access to such network facilities and software is also controlled by the use of secure passwords which must be changed on a regular basis.

All University staff PCs and laptops must be set with an inactivity screensaver which requires a unique password to reactivate the underlying session and has an idle time of no more than 10 minutes before activation.

As a means of allocating appropriate software packages to specific users, the use of an application deployment tool should be used. This can grant individuals or groups access to various programs and services in accordance to their duties and requirements through their user account.

Software Development

Where software development is outside of a course of study or University sanctioned activities or research, the development must only be performed in a controlled, test environment until such time that all flaws, bugs and potential vulnerabilities are removed. Only then can the developed software be applied to a production environment.
Software development, where not part of a course of study, should only be done where required, and for the purpose of enhancing an existing application or meeting a need where no commercial software exists for the purposes required. There may also be instances where it is cheaper, faster or more appropriate to perform the in-house development.

Any software development that may cause harm or impact the ITS resources of FedUni in an adverse manner including, but not restricted to, scanning, gaining un-authorised access, exploiting vulnerabilities to take advantage of exploits, will be looked upon as inappropriate and treated as a direct attempt to compromise the University computing facilities and / or infrastructure and will be dealt with accordingly.

End-Point Security and Antivirus Software

All SOE University issued PCs and laptops have end-point security software installed which has an automatic pattern update feature enabled. This is to ensure that the software is kept updated for the latest threats. There are also antivirus systems in place checking all incoming email into the organisation and also on internally circulating emails.

It is expected that any non SOE or University PCs and / or laptops also have current updated antivirus software installed, and it's the owners / users responsibility to ensure this. Not having current updated antivirus software installed exposes the University systems and infrastructure to potentially significant disruption and damage due to virus infected computers.

Passwords

It is essential that those requiring access to the University computing facilities be issued with a unique login and password. This password is not to be shared with, or used by, any other individual and failing to comply will be treated as a serious breach of system security which may result in disciplinary action.

Staff Passwords are to meet complexity rules as set by the Identity and Access Management System. These complexity rules will include a minimum password length, character requirements and suitable password expiry period.

In the event that access is required to University data that is held under a specific staff members user id and password and that staff member is unavailable to access the data due to unforeseen circumstances, a request to have the password reset may be made with the authorisation of the Vice Chancellor or delegated officer. This will only be considered when all other avenues to access the data have been exhausted. At the completion of the task accessing the required data, the password MUST be reset again and the staff member notified as soon as is practical.

Student Passwords are to meet complexity rules as set by the Identity and Access Management System. These complexity rules will include a minimum password length, character requirements and will NOT include an expiry date as student passwords have no requirement to expire at regular intervals. However, students will be encouraged to change their passwords on a regular basis.

Patch Management

To ensure that all FedUni supplied desktop operating systems and applications are kept current and up-to-date, a central Patch Management Server will be used. This server will send out any operating system and / or software updates, to FedUni supplied PCs and laptops, that are required to address any known software vulnerabilities. These updates will be distributed at the discretion of ITS Services.
It will be the responsibility of system administrators to ensure that the servers under their control are kept updated with required operating system and software updates and patches. Periodic checks will be performed on servers to assess their vulnerability status by the Information Security Officer in consultation with system administrators.

**Data Security**

Ensuring that the confidentiality of data contained on the information technology systems is maintained and access is made available to those who are authorised to see that data. This item should also be used in conjunction with confidentiality policies.

**Confidential Data Security**

To ensure the confidentiality and security of staff and student personal information contained on the Universities ITS facilities, it is essential that only those authorised to access such data are permitted to do so. Those who are permitted to access such information are granted appropriate access, as required by their job functions, by Student Systems and Processes or Human Resources.

Anyone, staff or student, who gains access to such personal information through methods other than those granted by Student Systems and Processes or Human Resources, shall be deemed as unauthorised and subject to disciplinary action.

Staff should be aware of their legal and corporate responsibilities in relation to appropriate use, sharing or releasing of information to another party. Any other party receiving restricted information must be authorised to do so and that the receivers of the data also adopt information security measures to ensure the safety and integrity of the data.

**Communications Security**

Communications can take various forms which include, but are not restricted to, voice via land line, voice via mobile phone, voice via computer network (VOIP), email, electronic file transfer, wireless access, Virtual Private Network (VPN) connections, dial up modem, Infra-Red, Bluetooth and ITS network infrastructure.

Each of these communications methods poses its own unique security problems and needs to be addressed individually. In each case, where network communications is required, irrespective of type, only those methods as permitted by ITS Services will be allowed and must be in accordance with the specific Communications Security procedures which are developed to support this policy.

**Physical Security**

Ensure that the physical ITS devices are kept safe from inappropriate access. This includes the physical access to the server room, switch and patch panel cabinets, and any other ITS devices in both restricted and public access areas.

**ITS Asset Control**

All ITS devices over a specified value must be registered with the University asset register. This also applies to the disposal of assets.

**ITS Asset Disposal**
When disposing of ITS assets such as computers, laptops, printers etc, the disposal must be co-ordinated with ITS Client Services to ensure that all data is removed using approved data removal tools and procedures. It is also a requirement that all software be removed prior to disposal to prevent potential breaches of software licence agreements.

Physical Access Security

All offices, computer rooms and work areas containing confidential information, or access to confidential information must be physically protected. This means that during working hours, the area must be supervised, so that the information is not left unattended, and after hours, the area must be locked or the information locked away.

It is a requirement that any PC / Laptop / Portable computer be logged out and turned off at the end of the working day unless a specific request is made to leave equipment turned on for the purpose of distribution of overnight processing is required.

Building Access

The following controls must be applied to restrict building access:

a. Access to computer work areas must be restricted by keys, cipher locks or proximity access cards during office hours and can only be accessible by authorised individuals after hours.

b. Combinations or access details must be changed / deleted when a staff member leaves or loses their card or key.

c. If door and keys have been used for other purposes, key cylinders must be replaced with a brand new lock and keys restricted to an absolute minimal number of persons.

d. Access to restricted computer work areas can only be given when an authorised staff member is inside and can and will supervise the visitor's movements completely or hand over to successive staff.

e. When unattended and after hours, doors must be secured.

f. Individual computer labs must be protected by timed door locks and also video surveillance.

Other workers must not attempt to enter restricted areas in FedUni buildings for which they have not received access authorisation

Removal of Equipment

No computer equipment can be removed from the University premises unless specific authorisation has been received by the school or section head or ITS Services. This does not apply to laptop or notebook computers where one of their primary purposes is to allow the custodian to work while away from their normal working location.

Any equipment taken from a FedUni campus without appropriate authorisation will be in direct violation of this policy and appropriate misconduct and / or legal action will be taken.

Physical Issue of Portable ITS Equipment

Any physical issue of FedUni portable equipment must have authorisation from the custodian with ITS Services informed. Persons who are issued such equipment must agree to personal responsibility of the equipment. When not in use, all portable ITS equipment must be secured.
Mobile / Portable and Hand Held Devices

Specific issues relating to resources such as, but not limited to, iPhone, Smart Phones, PDAs, iPad, mobile phones, laptop or notebook computers and the like and their use within the general system infrastructure.

Allowing Access

Any non FedUni issued laptop or portable device connected to the University network is the responsibility of the owner. FedUni will take no responsibility for virus or other damage that may be caused by being connected to the network.

Since portable and hand held devices are more and more common, it is necessary that we allow for their use on the network. All new staff laptops will be passed via the Information Technology Services section, or designated technical staff, for initial setup and testing to ensure that all the correct anti-virus and patch updates are installed and can be used safely on the network.

ITS Services will not be obliged to enter into any other support arrangements for non University owned devices.

Student laptops and other portable devices can be connected to the network only if they have current and updated end-point security software. These devices should only be connected to the network in authorised Public Access areas on the campuses. The reason being, that these Public Access Areas can be monitored and protected by ITS who can remove any devices that may be suspected of inappropriate activity.

Use of mobile devices on the University network are also subject to the Use of Computing and Communication Facilities policy.

Wireless Network Access

In keeping up with current networking trends and requirements, FedUni have adopted the use of wireless networking technology. In order to access the wireless networking facilities, portable equipment must first meet a strict security criteria as enforced by the use of an SSL/VPN device.

The use of wireless networking not supplied by FedUni will be deemed inappropriate and will be removed from the network unless provided by schools as part of a course of study. In such cases, the wireless network must be confined to a limited area such as a class room or lab and pre-approved by ITS Services.

Accepted Usage

It is expected that the custodians of laptops or other portable device will still abide by this policy and all supporting documents. Any breaches of this policy may lead to disciplinary action being taken.

Security Incident Management

Specify how any breaches of security relating to the information systems will be identified and handled.

Reporting Security Problems

Any suspected inappropriate or illegal usage of FedUni Information services network and equipment should be reported to the Service Desk or to a school or section head immediately. This information will then be reported to the Information Security Officer for investigation.
Emergency Plans

Disaster Recovery Plans, Business Continuity Plans, backup strategies and fail over plans for the core FedUni ITS services and infrastructure are the responsibility of the ITS Services to ensure that any outages or disasters can be recovered from in the shortest possible time with a minimal amount of data or resource loss.

These documents must include step-by-step instructions for the restoration of each service to ensure that, if required, other personnel from the ITS Services are able to perform the recovery. These documents also form part of the University Business Continuity Plan.

Escalation

The escalation process for the rating of each reported event will be determined by the relevant ITS Services staff member in conjunction with the Information Security Officer taking into account the event itself and other priorities at that time.

Monitoring and Reporting

Staff nominated by the Deputy Vice-Chancellor (Student Support & Services) will be authorised to monitor all aspects of the University network and associated infrastructure. They are also able to report any suspected inappropriate and / or illegal activity to the Information Security Officer in the first instance for further investigation in accordance with FedUni Incident Investigation procedures.

It is also the role of the Information Security Officer to actively monitor and analyse all network related activity included, but not restricted to, Internet Usage, email and dissemination and use of programs and data across the University network infrastructure.

This monitoring will be done for the sole purpose of identifying and responding to any suspected inappropriate activity.

"The content of e-mail and other electronic communications will only be accessed by the Information Security Officer-
1. after approval has been obtained from the Vice-Chancellor or delegated officer; and
2. if the access is permitted by law."

All information reported to the Information Security Officer shall be treated in the strictest confidence. Any reported information will be logged and relevant action taken, including reporting to relevant School or Section heads and other management as required.

Business Continuity

How to ensure that there will be minimal disruption to ITS services in the event of a disaster or the implementation of changes to systems and/or associated infrastructure.

Backup Requirements

All major systems within the University computing infrastructure are backed up on a regular basis. Information Technology Services have a Backup Strategy which details the frequency of backups. It is also strongly advised that all users save their work to their network drive as this drive is backed up and any loss or damage to files can often be rectified by the restoration of the files from an existing backup.
Change Control

To ensure that the ITS facilities and services running within the University infrastructure are maintained and kept running at maximum performance and functionality, it is often a requirement to perform maintenance and upgrades to equipment. To ensure that there is minimal disruption to essential services, appropriate Change Control procedures are to be followed. This is to ensure that the disruption is kept to a minimum and appropriate roll back procedures exist should there be issues during the system changes.

Disaster Recovery Plans

In the event of a disaster that impacts the ITS infrastructure and/or services, the implementation of a Disaster Recovery Plan is essential. The DRP provides step by step procedures and processes required to ensure that services are returned to normal operation in the shortest possible time. The production and maintenance of such plans are the responsibility of the various ITS staff assigned to any aspect of the network and ITS services.

Breaches / Infringements

Failure to abide by these terms will be treated as misconduct.

Minor Infringements

For a first time offence of a minor infringement, a warning will be issued. A second time offence will result in automatic denial of access to one or all facilities for a period of three (3) working days and up to two (2) weeks.

Serious Infringements

A serious infringement includes, but is not limited to, a third and subsequent offence of a minor infringement and will result in automatic denial of access to one or all facilities and will be referred to the Deputy Vice-Chancellor (Student Support & Services). This may result in:

- A prolonged denial of access to one or all facilities;
- Referral to the appropriate disciplinary procedures; and/or
- Referral to law enforcement agencies (where the infringement constitutes a legal offence).

Responsibility

The Deputy Vice-Chancellor (Student Support & Services) is responsible for the review and implementation of this policy and the maintenance of all associated documents.

Legislative Context

- Victorian Information Privacy Act 2000

Associated Documents

- Use of Computing and Communication Facilities Policy
Implementation

The “Information Security” Policy is to be implemented throughout the University in the form of notices via:

1. an ITS Announcement to all the University Staff;
2. an announcement under FedNews webpage;
3. Inclusion in the University's Policy Library.