INFORMATION SECURITY POLICY

Policy number	TEC 1.05
Policy name	Information Security Policy (Issue Three)
Applicability	Bond University Staff, students and users of the University's ICT resources
Policy owner	Director, Information Technology Services
Contact person	Director, Information Technology Services
Policy status	Approved Policy
Date of approval	29 November 2007
Date last amended	3 October 2017
Date last exposed	
Date last reviewed	
Date of next review	3 October 2020
Related policies	Staff Acceptable Use of ICT Facilities Policy (TEC 1.04) Student Acceptable Use of ICT Facilities Policy (TEC 1.01) Privacy Policy (COR 1.01)

1. OVERVIEW

Bond University recognises the importance of its ICT resources in supporting its teaching and learning, research and other administrative business processes. The security of these ICT systems must be managed accordingly to assist the University to meet its obligations in relation to the confidentiality, integrity and availability of information, including ensuring appropriate responsibilities and processes for information security.

This Policy forms the foundation for information security at Bond University to be used by all University staff, students and users of the University's ICT resources.

The purpose of this Policy is to ensure:

- appropriate availability of ICT resources;
- the integrity and validity of data;
- that ICT resources can be recovered effectively from disruption; and
- the protection of data, software and hardware components of the University's ICT resources.

Within this Policy, ICT resources include:

- Information assets (e.g. databases, files, training materials);
- Software assets (e.g. applications, systems software, and development tools); and
- Physical assets (e.g. computers, communications equipment and magnetic media).

The Policy applies to all users of the Bond University's ICT resources and provisioned services.

2. THE POLICY

2.1. Access Management

All users of Bond University's ICT resources must be authorised to access the appropriate systems. Access is controlled and monitored in accordance with University policy. The elements involved in controlling and monitoring access include:

- Identification;
- Authorisation; and
- Authentication.

2.1.1. Identification

All system users are assigned a unique username to use in accessing Bond University's systems and applications. Usernames must not be shared. Users are responsible for maintaining the security of their usernames and all activity occurring under those usernames. Usernames are issued in accordance with approved standards.

A limited number of generic user accounts are used for specific operational purposes by Information Technology Services. All generic accounts must be approved by the Director, Information Technology Services and a register of these accounts are maintained by Information Technology Services.

A limited number of anonymous access email terminals are also available in general use student areas that allow students to access the internet without requiring a Bond University Network Account.

2.1.2. Authorisation

Only those users who have valid reasons (as determined by the Operations Contact persons) for accessing the University's systems and information are granted access privileges appropriate to their educational and/or business requirements. Access is granted by means of a network account, which also serves as identification. Accounts are issued in accordance with approved standards.

2.1.3. Authentication

Each username requires a password for validating identity. Standards apply to all systems requiring authentication (refer to Password Management Procedures).

2.1.4. Account Management

All Operations Contacts and Applications Custodians must regularly review their system to determine who is authorised to use the system and their level of authorisation.

A six-monthly review of all system access levels of users should be carried out by the Operations Contacts and Applications Custodians. The purpose of the review is to ensure any non-compliance as a result of this activity is addressed as a matter of priority. All records of non-compliance must be kept by Information Technology Services until all matters arising from non-compliance have been resolved.

2.1.5. Privileged Users Access

System Administrators and Privileged Users will abide by Bond University Acceptable Use Policies and any other polices relevant to their employment.

Contractor and third-party access are permitted only if agreed to by the Operations Contact persons and a full-time employee sponsors the individual. These parties must comply with access control standards that require, at a minimum, that a unique username identify each user. This would then ensure that only authorised individuals receive access to systems. All temporary accounts should have an expiration date based on contract completion date.

2.2. Asset Security Management

2.2.1. Backup

All critical University information must be backed up on a regular basis. Backup schedules should include one full weekly backup, and six incremental backups.

2.2.2. Recovery

All backups of critical data must be tested periodically to ensure that they support full system recovery. System restoration procedures must be documented and tested annually. Backup media must be retrievable 365 days a year.

2.2.3. Off-Site Storage

Off-site is synonymous with "out of the building". The off-site storage location must provide evidence of adequate fire and theft protection and environmental controls.

2.2.4. Data Retention

Currently University Data is retained on a 17-week rotational basis. However, in addition to this schedule, a full database export of the finance system is performed before and after the year end processing and the data exports are retained for 7-year period.

2.2.5. Security

All major ICT resources must be accounted for and have a nominated Operations Contact who is responsible for the implementation and management of this Policy in relation to those assets.

2.2.5.1. Physical Security

Access to secure areas, including computer rooms, network equipment rooms and any associated service facilities, is restricted to authorised University staff, through the use of passwords, locks or access-control devices. All wiring closets must be physically secured

2.2.5.2. Data Security

Different types of data require different levels of security. The University classifies data into three categories: Public, Proprietary and Restricted. It is the Operations Contact who is responsible for

establishing authentication and authorisation guidelines for their ICT resources data. Please note that:

- Public data can generally be made available or distributed to the general public;
- Proprietary data is for internal University use and not for external distribution; and
- Restricted (moderately to highly sensitive) data is to be used only by individuals who require it in the course of performing their University responsibilities, or data, which is protected by Commonwealth and/or State legislation. Restricted data can only be deleted with the permission of the Operations Contact person.

Staff should be aware of their legal and corporate responsibilities concerning inappropriate use, sharing or releasing of information to another party. Any third party receiving Proprietary or Restricted information must be authorised to do so and that individual or their organisation should have adopted information security measures, which guarantees confidentiality and integrity of that data.

2.2.5.3. Software Security

Software, for the purpose of this Policy document, is defined as the programs and other operating information used by, installed on, or stored on University owned computer systems or storage media.

To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all licensing agreements must be adhered to. All software and other applicable materials must be licensed (if required) in an appropriate manner.

In order to comply with licensing regulations and to prevent software piracy, the purchasing and licensing of software and other applicable materials should be carried out through Information Technology Services.

All software, including patches, upgrades or new versions, should be tested, archived and documented before being put into production systems. This transition should be under migration and version control and incorporate ITIL change management principles. Control measures should also be in place for maintaining and accessing program and system source libraries.

All operational software should be maintained at current versions or at a level supported by the supplier. Processes should be in place to ensure that information systems development and operational environments for critical systems are separated logically from each other.

Software development policies and procedures will adhere to University best practice standards and guidelines.

2.2.5.4. Internet Security

Internet accessible systems must be approved by Information Technology Services prior to installation on the network. Internet accessible systems will be built according to University best practice standards and guidelines. Internet systems and services will be penetration tested annually to ensure continuity of security and integrity.

Bond University network traffic that egresses the Bond network to the Internet and external networks must either be routed via Bond University Web Gateway or be defined per protocol and port in the corporate firewall. Indiscriminate access to all TCP and UDP ports is not permitted. Requests for additional protocol and port access must be submitted via Information Technology Services Desk.

2.2.5.5. Mobile Equipment/Wireless Devices Security

Special usage policies and procedures will apply to mobile and wireless devices and are not detailed in this Policy - refer to Use of ICT Facilities Policies TEC 1.01 & 1.04.

2.3. Security Breach Notification and Reporting

2.3.1. Security Breaches

A security breach is defined as any action or event in contravention to the provisions of this Information Security Policy, relevant Bond University Policies and applicable State and Federal laws.

The guidelines listed under "notification" below, should be applied during the course of an actual or potential security breach.

2.3.2. Notification of a Security Breach

The following steps are listed in the order that they should be taken. Once a breach is confirmed, the responsible officer should take these steps as urgently as possible. If a particular step is not appropriate to the breach, then the officer should ignore it and move to the next step.

a) The Director, Information Technology Services should be notified immediately.

b) If the security breach involves a possible breach of State or Federal, law, then the Director, Information Technology Services or delegate will notify Queensland Police Service or Australian Federal Police (as appropriate), as soon as is practicable.

c) If a University business unit or Faculty is involved, then the appropriate manager or Executive Dean should be notified as soon as possible.

d) If an organisation or person external to the University is involved as a potential victim, then that organisation or person should be advised as soon as possible.

e) If an organisation or person external to the University is involved an assessment will be made by the Director, Information Technology Services as to whether the Australian Computer Emergency Response Team (AUSCERT) should be contacted.

2.3.3. Reporting a Security Breach

The person authorised by the Director, Information Technology Services, to carry out the technical investigation of a security breach must submit a report outlining the following details (where possible):

- General nature of the security breach;
- General classification of people involved in the security breach, (such as external client, privileged staff member);
- Systems involved in the security breach;
- Details of the security breach;
- Impact of the security breach;
- Unrealised, potential consequences of the security breach;
- Possible courses of action to prevent a repetition of the security breach;
- Side effects, if any, of those courses of action.

2.3.4. Unauthorised Access Attempts

This includes anything from harmless exploration to hacking in order to gain access to information. Unauthorised access also includes gaining access to computer systems for future use (e.g. extortion).

All unauthorised access attempts must be noted and logged. The Audit Trail/System Access Log must be reviewed regularly, exception reports generated and inspected by the System Administrator and appropriate action taken. A copy of the report of unauthorised access attempts must be produced and kept for future reference.

2.4. Access Control Standards

2.4.1. Identification Standards

Usernames will be issued in accordance with the following standards:

- Staff on acceptance of appointment are provided with unique usernames and passwords;
- Students on confirmation of enrolment are provided with unique usernames and passwords;
- Any other University approved and authorised users (e.g. casuals, volunteers and adjuncts) require the relevant Executive Dean/Manager to make application to Information Technology Services for access;
- Accounts designed for use by more than one person are not normally permitted. An exception to this can only be authorised by the Director, Information Technology Services;
- Guest login accounts are not normally permitted. A Guest login account will only be issued with the approval of the Director, Information Technology Services.
- Guest WiFi access will be exclusively provisioned for sponsored guests through a self-registration system and is facilitated by the Operations Contact.

All account creation or system access level requests must be authorised by the appropriate Executive Dean/Manager.

2.4.2. Authorisation Standards

Accounts will be issued in accordance with the following standards:

- Only the authorised user may use an account. A user is authorised to use an account if:
  - The user is the account holder (in the case of a user account); or
  - The account is a public access account; or
  - The Operations Contact believes such authorisation is warranted;

- An account holder will not authorise or allow the use of the account by other persons except where the Director, Information Technology Services grants permission for the account holder to allow such use of the account. Approval to allow the use of an account by persons other than the authorised account holder must be requested, in writing, from the Director, Information Technology Services (or delegate) through the relevant Executive Dean/Manager;
- A user will use an account only for approved activities;
- When the Operations Contact creates accounts for specific public facilities, the University owns these accounts. Users may use them only for the specified purposes;
- The user will not attempt to circumvent the security mechanisms of any ICT system unless authorised by the Operations Contact;
- The Operations Contact may decide to disable or remove accounts if the following events happen:
  - The account is no longer required by the account holder;
  - The account holder ceases to have an association with Bond University;
  - The account is inactive for a given period of time (e.g. six months);
  - The account is used for non-approved activities.

2.4.3. Authentication Standards

The following standards should be applied to all systems requiring authentication:

- Passwords must be used for accessing all corporate systems;
- Passwords must be at least eight characters in length;
- A newly-issued password must be changed as soon as possible after issue;
- Passwords must not be displayed in any form;
- When logging on, users shall take precautions to ensure others do not see their password;
- Passwords must not be disclosed to others;
- Passwords must not be easily associated with a particular user;
- Users must not save passwords electronically within applications;
- A user who suspects that a password has been compromised shall change the password, if possible. The user is required to report all details of the suspected breach to the Director, Information Technology Services.

Where possible, all passwords should be stored in an encrypted format on systems.

2.5. Asset Security Standards

2.5.1. Internet Security Standards

The following are the minimum accepted standards for protection of Internet capable devices operating on the Bond University network:

- A firewall, or equivalent, will be used between the Bond University Corporate Network and the Internet;
- Only explicitly permitted traffic is allowed through the firewall, or equivalent. All other traffic is rejected;
- All traffic passing through the firewall must be capable of being logged and audited;
- All Internet/Web servers which require connectivity to the Bond University network must be approved by the Director, Information Technology Services or designate;
- All Internet/Web servers will be built and configured in accordance with Bond University best practice standards and guidelines.
- Use will be for University-related and approved purposes.

2.5.2. E-mail Security Standards

The following are the minimum acceptable standards for the use and management of e-mail within the University's information management and technology environment:

- A password must be used on all e-mail systems;
- The use of scanned signatures should be discouraged;
- E-mail that is non-business related should have a disclaimer that the opinions are an individual's and not those of the University;
- Staff email communications are University assets and are not private correspondence;
- E-mail systems should be backed up and maintained in accordance with backup and recovery standards**;**
- Staff will use the standard email signature template as approved by Bond University Marketing Department;
- Third party vendors sending e-mails on behalf of the bond.edu.au domain should be approved by Information Technology Services and conform to appropriate standards.

2.5.3. Backup and Recovery Standards

The following are the minimum acceptable standards for backup and recovery of the University's information resources:

- Backup cycles should be related to the business risk, frequency with which data and software is changed and criticality of the system to business operations;
- A register of backups, including verification of their success, should be maintained;
- A cycle of backup media should be used for all backups, with at least one copy of each cycle stored off-site;
- In addition to above, a system backup should be performed before and after major changes to the operating system, system software or applications;
- Consideration should be taken when upgrading technologies to ensure that backup data is able to be read in the new environment;
- Regular tests of key corporate systems backup data should be performed (in a safe environment) to verify that the system can be recovered from backups produced;
- A cycle of backup media should be retained of all information required to meet customer service, legal or statutory obligations;
- Operator logs should be maintained, monitored and reviewed on a regular basis; to ensure that correct computer operating procedures have been complied with.

2.6. Operational Security Guidelines

2.6.1. Documentation Operating Procedures

The following are minimal acceptable standards for documenting operating procedures and processes:

- User manuals should be maintained on all current hardware, software applications and in-house developed systems;
- Authorisation processes for approving all changes to corporate information facilities including operating systems, software applications and hardware should be in place;
- Procedures should be in place for recording and monitoring of security violations and exposures.

2.6.2. Change Control

The following are minimal acceptable standards for documenting Change Control:

- Ensuring adequate testing and change control mechanisms are in place for the migration of new or modified systems into the operational environment;
- Ensuring that the information environment is managed so that future expansions or changes can be accommodated and do not adversely impact the operational environment.

2.6.3. Malicious Software

The following activities are the minimum acceptable standards for controlling and mitigating malicious software:

2.6.3.1. Virus and Intrusion Detection, Prevention and Scanning

- All University owned staff and student personal computer equipment should have the current version of anti-virus software installed;
- Anti-virus software should be configured in "real-time" mode to ensure any infections are identified and cleaned immediately upon detection;
- Anti-virus software should be regularly updated with new definition files;
- All incoming and outgoing e-mail attachments should be scanned. If a virus is detected, the attachment should be cleaned before distribution. If not, then the message and attachment should be blocked and the sender notified;
- Anti-virus software should be regularly reviewed, as it may be necessary to use more than one type of scanning software to ensure that maximum protection is provided for all information platforms and environments;
- All data traversing the University owned network is susceptible to random inspection for the purposes of identifying, monitoring and controlling threats. Only authorised staff members, with the approval of the Director of Information Technology Services, shall perform such activities.

2.6.3.2. Education and Awareness

- Regular communication should be sent to users alerting them of potential virus or network attacks. Users should be educated about malicious software in general, the risks that it poses, virus symptoms and warning signs including what processes should be followed in case of a suspected virus;
- Users must be made aware that the installation and use of unauthorised software on University owned assets is prohibited.

2.7. Enforcement

Bond University considers any breach of security to be a serious offence and reserves the right to copy and examine files or information resident on or transmitted via the University's ICT resources. Students deemed to be in breach of security are subject to disciplinary action. Staff deemed to be in breach of security are subject to disciplinary action available under industrial provisions. Offenders may also be prosecuted under State, Commonwealth and International laws.

Information Technology Services may remove material from ICT systems or services or close any account that is endangering the running of the ICT resource or that is being exploited for inappropriate or illegal use.

Information Technology Services may remove from the network, without notice, any system that is deemed as being exploited for inappropriate or illegal use or is disrupting the delivery of University services.

2.8. Awareness and Communication

It is essential that all aspects of information security, including confidentiality, privacy and procedures relating to system access, should be incorporated into formal staff induction procedures and conveyed to existing staff on a regular basis.

Each employee, on commencement of employment, should be made aware that they must not divulge any information that they may have access to in the normal course of their employment. Staff must also be made aware that they should not seek access to data that is not required as part of their normal duties.

Appropriate information and system security training should be provided to relevant employees as required.

3. DEFINITIONS

Operations Contact:	The key person nominated within the business unit who is the point of contact for any issues or information related to how the system is used from a business perspective.
Applications Custodian:	The key person nominated within Information Technology Services who is the point of contact for any issues or information related to the technical operation of a system.

4. RELATED PROCEDURES, GUIDELINES AND FORMS

Password Management Procedures

PASSWORD MANAGEMENT PROCEDURE

1. Overview

The purpose of this Procedure is to establish a standard for the creation of secure passwords, the protection of passwords, and the frequency of password change.

Passwords are an important aspect of information security. They are the front line of protection for most computer systems. A poorly chosen password may result in the compromise of the Bond University corporate network. As such, all Bond University staff (including all third parties such as contractors and vendors with access to Bond University systems) are responsible for taking the appropriate steps, as outlined below, to ensure their passwords are secure.

Bond University uses a role-based approach for password management. Based on their role in the University, each staff member will be assigned to a security profile, and each security profile has an associated password guideline. If an individual has several roles, with conflicting password guidelines, the "strongest" guideline applies.

2. General

a) Three levels of password guidelines are used, each with a different set of requirements for password creation and reset, and these are described in the password guideline matrix.
b) The assignment of a password guideline is based on an individual's role(s) at the University and is not an automatic result of an affiliation or staff position.
c) All passwords must be changed as per the password guideline matrix. This will be enforced at the operating system level i.e. Windows, and at the application level, where possible (this will be dependant on system capabilities).
d) Passwords must not be inserted into email messages or other forms of electronic communication.
e) Password guidelines and security roles, and the resulting association of password guidelines to a user, are managed by Information Technology Services.

3. Password Protection Standards

All passwords are to be treated as sensitive, confidential Bond University information. The following password standards should be adhered to:

a) Do not reveal a password over the phone to ANYONE;
b) Do not hint at the format of a password (e.g., "my family name");
c) Do not reveal a password on questionnaires or security forms;
d) Do not share a password with family members;
e) Do not reveal a password to co-workers while on vacation;
f) Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer);
g) Do not store passwords in a file on ANY computer system (including mobile devices) without encryption;
h) Temporary passwords should be changed at first log on;
i) If a password has been compromised or there is a possibility it may have been compromised then users should change their password immediately.

4. Application Development Standards

Application developers must ensure their programs adhere to the following security guidelines:

- Applications should support authentication of individual users, not groups;
- Applications should not store passwords in clear text or in any easily reversible form;
- Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

5. Exclusions

- Infrequently there are certain circumstances whereby a particular vendor, technology or business process is unable to comply with this policy.
- Information Technology Services reserves the right to approve exceptions through a case-by-case review process, requiring final sign-off from either the Information Security Manager or Director, ITS.

6. Related Guidelines and Forms

Password Construction Guidelines and Matrix

PASSWORD CONSTRUCTION GUIDELINES

All Bond University Staff should ensure they select **strong** passwords. Strong passwords have the following characteristics:

a) Contain both upper and lower-case characters (e.g., a-z, A-Z);

b) Have digits and/or punctuation characters as well as letters (e.g., 0-9, @#$%^&*()_+|~-=\`{}[]:";'<>?,./);

c) Are at least eight alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e);

d) Are not words in any language, slang, dialect, jargon, etc.;

e) Are not based on personal information, names of family, etc.;

f) Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Poor or weak passwords have the following characteristics:

a) The password contains less than eight characters;

b) The password is a word found in a dictionary (English or foreign);

c) The password is a common usage word such as:

   i. Names of family, pets, friends, co-workers, fantasy characters, etc.;

   ii. Computer terms and names, commands, sites, companies, hardware, software;

   iii. The words "Bond University", "Robina", "Gold Coast" or any derivation;

   iv. Birthdays and other personal information such as addresses and phone numbers;

   v. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.;

   vi. Any of the above spelled backwards;

   vii. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Password Guideline Matrix

Name	Description	Example
Level 0	Standard	Students, Vendors/Guests
Level 1	Medium	Staff
Level 2	High	Chancellery, PVCs, Executive Directors, Executive Deans, Faculty Business Directors (Typically all staff on executive contracts)

Attribute	Level 0	Level 1	Level 2
Minimum length of password	8	8	8
Maximum age of password (in days)	365	365	90
Days of daily expiration warnings	14	14	14
Password minimum age for reset (in days)	0	0	0
Password uniqueness/history	5	5	5
Failed attempts before lockout	5	5	5
Password Complexity	False	True	True