INFORMATION SECURITY POLICY

Policy number	TEC 1.05
Policy name	Information Security Policy (Issue Four)
Applicability	All users of Bond University's ICT resources.
Policy owner	Director, Information Technology Services
Contact person	Information Security Manager, Information Technology Services
Policy status	Approved Policy
Date of approval	29 November 2007
Date last amended	19 May 2021
Date last exposed	May 2021
Date last reviewed	
Date of next review	19 May 2024
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

The purpose of this Policy is to provide a security framework that ensures the protection of Bond University's information assets from Unauthorised Access, loss, or damage – while supporting its teaching and learning, research and other administrative business needs.

The security of Bond's Information must be managed accordingly to assist the University to meet its obligations in relation to the confidentiality, integrity and availability of information, legislative compliance obligations, and ensuring appropriate responsibilities and processes for information security.

2. WHO IS AFFECTED BY THIS POLICY

This Policy applies to all University faculty and staff, students, alumni, and those acting on behalf of Bond University through service on University bodies such as task forces, councils, and committees. It also applies to all other individuals and entities granted use of University Information, including, but not limited to, contractors, temporary employees, third parties and volunteers.

This Policy applies to all Bond Information assets, whether processed by Information Technology Systems or Services, or held in physical records sources, regardless of whether or not the processing or storage is undertaken by Bond. The Policy equally applies to cloud-based services used by Bond; voice and data communications equipment and Software used by Bond; research data; personal equipment connected to the Bond network; and Bond data stored at rest or in transit.

3. RESPONSIBILITIES

All Bond University faculty, staff, students and others granted use of University Information are expected to:

1. Understand the information classification levels defined in the Information Security Policy.
2. As appropriate, classify the information for which one is responsible accordingly.
3. Access information only as needed to meet legitimate business or academic needs.
4. Not divulge, copy, release, sell, loan, alter or destroy any University Information without a valid business or academic purpose and appropriate authorisation.
5. Protect the confidentiality, integrity and availability of University Information and immediately report any suspected breaches of information security.
6. Maintain awareness of the information security risks and controls appropriate to the information accessed and used, including completion of required training as required by the University.
7. Handle information in accordance with the Acceptable Use Policy and any other applicable University standard, procedure, guideline, or policy.

8. Safeguard any physical key, ID card, computer account, or network account that allows one to access University Information.
9. Managers of employees must ensure correct termination dates are entered into Bond's HR system for staff terminations to ensure the user account is disabled.
10. Discard media containing Bond University Information in a manner consistent with the information's classification level, type, and any applicable University retention requirement. This includes information contained in any hard copy document (such as a memo or report) or in any electronic, magnetic, or other storage medium (such as a memory stick, hard disk, etc).
11. Contact the Office of the General Counsel prior to disclosing information generated by that Office or prior to responding to any litigation or law enforcement subpoenas, court orders, and other information requests from private litigants and government agencies.
12. Contact the appropriate University office prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.
13. Be aware of all 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.

4. THE POLICY

4.1 Classification Levels

All University Information is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information.

When combining information, the classification level of the resulting information must be re-evaluated independently of the source information's classification to manage risks.

Data classification	Description	Examples
Highly sensitive	Data that if breached due to accidental or malicious activity would have a **high** impact on the University's activities and may cause serious harm to individuals. Dissemination is based on strict activity, research, or business need.	▪ Data subject to regulatory control (for e.g., research data) ▪ Individually identifiable Medical records ▪ Credit card details ▪ Tax file numbers ▪ Passport numbers ▪ Criminal and legal proceedings ▪ Passwords, PINs, system credentials and encryption keys ▪ Details of cybersecurity reports, vulnerability assessments, penetration test results
Sensitive	Data that if breached due to accidental and malicious activity would have **medium** impact on the University's activities and objectives. Dissemination is based on strict activity, research, or business need.	▪ Student records or staff records ▪ Organisational financial data ▪ Examination materials and results ▪ Pay information ▪ Staff performance (PDR) and eTEVALs
Private	Data that if breached due to accidental or malicious activity would have a **low** impact on the University activities and objectives. Dissemination is based on academic, research or business need.	▪ Business unit procedures or processes ▪ Contracts ▪ Course and unit performance information ▪ Key performance Indicators
Public	Data that if breached due to accidental and malicious activity would have **insignificant** impact on the University's objective	▪ Faculty and staff directory ▪ Course and unit information ▪ Organisational charts ▪ Published research data

4.2 Access Management

Logical and physical access to Bond's information assets must be authorised, controlled, and used in accordance with University policy, as follows:

1. All Bond systems, and systems storing Bond's information assets, must be protected against improper access.
2. Access to Bond's information assets and systems is granted by means of a network account, which also serves as identification. Accounts are issued in accordance with approved standards.
3. All system users are provided a unique user account to use in accessing Bond University's systems and applications. User accounts and access credentials must not be shared and must only be used by the person for whom the account has been created.
4. Each user account requires a password and/or other access credentials to validate the user's identity.
5. Passwords must be changed immediately if there is a suspicion of compromise.
6. Users are responsible for maintaining the security of their accounts and all activity occurring under those accounts. Knowingly disclosing passwords or other access credentials to others will be deemed a breach of policy and could be referred to disciplinary procedures.
7. Passwords used on all systems should comply with Bond's Password Management Procedures to ensure appropriate protection of Bond's information assets.
8. Access to Bond's information assets is granted on the "least privilege" principle, whereby each user should only be provided access to meet legitimate business needs and is granted the most restricted set of privileges needed for the performance of relevant business tasks.
9. 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 or insurance certificate of currency expiry date, whichever is sooner, must be used to ensure the temporary account is not accessible after that date.
10. Each non-temporary staff user account is disabled on termination of employment, and each non-alumni student account is disabled at the end of being an enrolled student.
11. Multi-Factor Authentication is required for remote access to Bond University's systems.
12. Applications Custodians must regularly review their systems to determine who is authorised to use the system and their level of authorisation. All records of non-compliance must be kept by Information Technology Services until all matters arising from non-compliance have been resolved.

4.3 Information Asset Management

The protection of Bond's information, application and technology assets are paramount to the integrity and availability of information, in accordance with the following:

1. University Information assets must not be sent to, exported to, nor stored on a non-Bond managed computer system, such as a home computer.
2. University Information assets must be appropriately protected when stored, transported, or transmitted.
3. University Information assets must be properly disposed of so that the information cannot be retrieved or reassembled when no longer needed or required to be kept under retention obligations.
4. University Information assets must be stored on Bond sanctioned storage, which includes Bond file servers, Bond corporate cloud storage and Bond managed systems – but not on local computers, USB, or other removable devices, or in personal (non-Bond) cloud services.
5. To the extent that any information system or service that stores, hosts, or processes any data that contains any confidential or Personal Information (as defined in the Privacy Act 1988), that data should be hosted in Australia, unless exempted by the Director ITS.
6. Bond systems and information assets must be backed up on a regular basis and backups must be tested periodically to ensure that the procedures followed support full information recovery.
7. Email communication from any system or software must be sent from, or forged with, an approved @bond.edu.au sender address, or sent via Bond's authenticated SMTP using TLS.

4.4 Physical Security

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

4.5 Software Security

1. 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.

2. In order to comply with licensing regulations and to prevent software piracy, the purchasing and licensing of all software and other applicable equipment or materials must be carried out through Information Technology Services.
3. All software, including patches, upgrades, or new versions, must be tested, archived and documented before being put into Production systems. This transition should be under migration and version control and incorporate appropriate change control procedures. Control measures should also be in place for maintaining and accessing program and system source libraries.
4. All operational software should have appropriate support in place by the supplier to ensure regular maintenance, adherence to current security standards and compliance with Bond's patch management procedures.
5. Processes should be in place to ensure that information systems development and operational (Production) environments for critical systems are separated logically from each other.
6. Systems that manage user passwords must be designed in such a way that the passwords are not retrievable by administrators.
7. All Bond systems and software must not be used in a manner that violates University policies.

4.6 Internet and Third-Party Accessible Security

1. 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, guidelines, and procedures. Internet systems and services will be penetration tested annually to ensure continuity of security and integrity.
2. 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 to Information Technology Services.
3. Bond must conduct appropriate due diligence on third parties that will process, store, host or have access to Bond information assets or sensitive systems.
4. Contracts with vendors that manage information assets or systems must contain specific confidentiality and security language already approved by Bond's General Counsel or be reviewed the General Counsel.
5. The security design, policies, and procedures of vendors and other third parties who will collect, process, host or store Bond's information assets or manage Bond critical systems must be reviewed by Bond's Information Security team.
6. In the case of ongoing maintenance and support from 3rd parties, access must only be granted to the relevant facilities within the system and be restricted to only the systems for which they provide support.

4.7 Device Security

1. All devices (including desktops, laptops, servers, virtual machines, and mobile devices such as smartphones and tablets) storing or processing Bond information must meet Bond's device and information protection requirements.
2. All devices connecting to or installed on a non-guest Bond network or authenticating to Bond systems must be configured and maintained for secure operation, including but not limited to:

    a) Non-default unique passwords/credentials that limit access to authorised individuals and services;
    b) Device must support current enterprise grade network protocols and be properly registered on the network;
    c) Compliance with Bond's patch management procedures. Current and supported operating system (firmware and software), regular updates and patching of firmware and software;
    d) Encrypted storage where supported, and protections against installing or running malicious software where technically feasible.
3. The information stored on the device must be protected against access if the device is lost, stolen, or recycled/reissued to another user. All mobile devices (laptops, tablets, mobile phones, etc.) and workstations that may be used to store or access Bond information, including accessing Bond email, must be securely configured, including automatic locking after a period of inactivity, and encryption of data stored on the device, where this feature is supported.
4. Mobile and portable devices should have Mobile Device Management (MDM) in place to facilitate remote wiping, encryption and other hardware controls.

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 & TEC1.04.

4.8 Information Security Audits and Monitoring

The University maintains logs and audit trails of network and system activities which may include personal information about users.

The Information Security Team at Bond performs information security audits and monitoring activities which include the following:

- monitoring its network, information systems, and services against malicious activities, and threats;
- logging and investigating its network, applications, and user activities for the purpose of investigating faults or problems, security breaches, and unlawful activity; and
- regularly auditing the security of information systems and reporting to appropriate University committees, including the Audit and Risk Management Committee.

Where diagnosis of problems, investigations or security audits are required, the University reserves the right to access logs, audit trails and individual files. In carrying out these tasks, cooperation with the Information Security team may be required. Cooperation and collaboration with law enforcement authorities may also be required.

4.9 Security Breach Notification and Reporting

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.

Any actual or suspected loss, theft, or improper use of or access to confidential information (or a device storing confidential information) must be reported promptly. The responsible officer should take these steps as urgently as possible:

1. The Director, Information Technology Services should be notified immediately;
2. Complete Bond University's Data Breach Response Plan to assess whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity;
3. If the security breach involves a possible breach of State or Federal law, then the Director, Information Technology Services or delegate will notify the Australian Cyber Security Centre or Australian Federal Police (as appropriate), as soon as is practicable;
4. If a University business unit or Faculty is involved, then the appropriate manager or Executive Dean should be notified as soon as possible;
5. 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.

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.

An assessment will be made by the Director, Information Technology Services as to whether the Australian Computer Emergency Response Team (AusCERT) or other external organisation will be engaged to investigate and assist with remediation.

5. BREACH OF POLICY

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.

Misuse of University digital information services or assets, or any other breach of this Policy and supporting procedures, may result in immediate suspension of an individual's User Account access. It may also be regarded as misconduct and dealt with under the relevant University processes.

A proven breach may result in disciplinary action, including termination of employment, contract, or enrolment. Offenders may also be prosecuted under State, Commonwealth, and International laws.

6. 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 Custodians:	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.
Personally Identifiable Information:	Personally Identifiable Information (PII) is information or an opinion about an identified individual, or an individual who is reasonably identifiable. For example, name, address, date of birth, age, gender, race, email address, tax/bank/credit information etc.
Software:	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.
University Information:	Information that Bond University collects, possesses, or has access to, regardless of its source. Comprises all forms of data or knowledge, in document or raw data form, that are processed, stored, and transferred that have value to the University in electronic or hard copy forms.
Unauthorised Access:	Looking up, reviewing, copying, modifying, deleting, analysing, or handling information without proper authorisation and legitimate business need. 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).

7. RELATED PROCEDURES, GUIDELINES AND FORMS

Password Management Procedures
Personal Cloud Storage Guidelines - ITS
Data Breach Response Plan
Enterprise Architecture Guiding Principles
Requesting Purchase of New Software - Checklist
Information Protection Guidelines