BOND UNIVERSITY	**INFORMATION SECURITY POLICY**
Policy Owner	Director, Information Technology Services
Contact Officer	Chief Information Security Officer, Information Technology Services
Endorsement Authority	Vice President Operations
Date of Next Review	20 March 2028

1. PURPOSE AND OBJECTIVES

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 privacy, confidentiality, integrity and availability of information, legislative compliance obligations, and ensuring appropriate responsibilities and processes for device and information security.

Information Assets storage include:

- Electronic data repositories, including on-premises or hosted servers.
- Physical repositories – including hardcopy files, USBs
- Data stored on Devices
- Data stored in SaaS and Software subscription services
- Data stored on telecommunications solutions

2. AUDIENCE AND APPLICATION

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

This Policy applies to all procured, subscription, free or developed solutions and equipment that access, store or process Bond information, whether in the cloud, stored electronically on-premise, or held in physical records sources, regardless of whether or not the processing or storage is undertaken by Bond. The Policy equally applies to research data; approved personal equipment connected to the Bond network; and Bond data stored at rest or in transit.

3. ROLES AND RESPONSIBILITIES

Role	Responsibility
Director, Information Technology Services	▪ Exemption for any information system or service that stores, hosts, or processes any data that contains any confidential or Personal Information data to be hosted outside Australia (clause 4.2(4)) ▪ Authorise all devices connecting to or installed on a non-guest Bond network (clause 4.6(1)) ▪ Approval to access, process, develop or store Bond Information on non-Bond managed devices (clause 4.6(4))
Chief Information Security Officer	▪ Authorise all devices connecting to or installed on a non-guest Bond network (clause 4.6(1))
Company Secretary & General Counsel	▪ Provide advice to staff who are required to respond to litigation or law enforcement subpoenas, court orders, and other information requests from private litigants and government agencies (clause 4(9)
All users of BU ICT resources	▪ Comply with the Policy and in particular the Policy Principles (clause 4) ▪ Promptly report suspected Cyber Incidents to cyber@bond.edu.au or the IT Service Desk (clause 4.8(1))

4. POLICY PRINCIPLES

All Bond University faculty, staff, students, Alumni and others who access, process or develop Information are expected to:

1. Access information only as needed to meet legitimate business or academic needs.
2. Not divulge, copy, release, sell, loan, alter or destroy any University Information without appropriate authorisation.
3. Not store Bond information assets on personal devices or within personal software subscriptions.

4. Protect the confidentiality, integrity and availability of University Information and immediately report any suspected breaches.
5. Maintain awareness of the information security risks, guidelines, and controls appropriate to the information assets accessed, created and used, including completion of required training as required by the University.
6. Handle information in accordance with applicable University standards, procedures, guidelines, or policies.
7. Safeguard any physical documents, USBs, keys, ID card, computer account, or network account that allows one to access University Information.
8. Discard media containing Bond Information in a manner consistent with the Information Protection Guidelines and Bond retention and disposal requirements. 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).
9. 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.
10. Contact the appropriate University office prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.
11. 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.
12. Ensure the completion of a Privacy Impact Assessment (PIA) is completed for systems that store Personally Identifiable Information (PII).
13. All development of information assets completed by Bond staff or on behalf of Bond to adhere to Information Technology Services development guidelines.
14. Ensure there is an understanding of the Information Protection Guidelines and the application for these classifications to data access requirements. And as appropriate, classify the information for which one is responsible for accordingly.
15. Complete any compulsory security and or privacy training.

4.1 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 an IT account, which also serves as identification. Accounts are issued in accordance with approved standards.
3. All system users are provided a unique IT account to access Bond University's systems. 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 IT 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 Procedure 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. Staff IT accounts are disabled on termination of employment, and each non-alumni student account is disabled at the end of being an enrolled student. See IT Account Termination Procedure for more information.
11. Multi-Factor Authentication is required for access to Bond University's systems and data.
12. Applications Custodians must regularly review their systems to determine who is authorised to use the system and their level of authorisation.
13. All records of non-compliance must be kept by Information Technology Services until all matters arising from non-compliance have been resolved.

4.2 Information Asset Management

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

1. University Information Assets must be stored on a 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) devices or cloud services..
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. 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.
5. 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.
6. 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 or signed with a DKIM key provided by Bond.

4.3 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.

4.4 Software Security

1. To ensure the security of Bond's data and to comply with licensing regulations, and reduce software supply chain risk, all software and subscriptions, regardless of cost, must be assessed and approved in accordance with the Software and Software Subscriptions Policy prior to use.
2. All software, including patches, upgrades, or new versions, must be tested, 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.
3. All software should have appropriate support in place to ensure regular maintenance, adherence to current security standards and compliance with Bond's patch management procedures.
4. Processes should be in place to ensure that information systems development and operational (Production) environments for critical systems are separated logically from each other.
5. All Bond Systems and software must not be used in a manner that violates University policies
6. All software to include advanced authorisation features such as Single Sign-on which includes multi-factor authentication.

4.5 Internet and Third-Party Accessible Security

1. Internet accessible systems and subscriptions must be approved prior to procurement and use, this includes free software.
2. 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.
3. 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.
4. Bond must conduct appropriate due diligence on third parties that will process, store, host or have access to Bond information assets or sensitive systems.
5. 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.
6. 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.
7. In the case of ongoing maintenance and support from 3rd parties, access must only be granted to the systems for which they provide support and for the period of support only.
8. Access to data in hosted solutions must be made available to Bond staff to download and archive.

4.6 Device Security

1. All devices connecting to or installed on a non-guest Bond network must be authorised by the Director, Information Technology Services or Chief Information Security Officer, and 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) Devices must support current enterprise grade network protocols;
    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
e) Anti-virus software.

2. The information stored on Bond managed devices must be protected against access if the device is lost, stolen, or recycled/reissued to another user.
3. All devices that are 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. Non-Bond managed devices must not access, process, develop or store Bond Information unless approval by Director of ITS provided. If a non-managed Bond device is approved, an MDM solution may be required on the device to enable wiping of any accidentally stored information if the device is stolen, lost or the staff member leaves Bond employment.

4.7 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 network, information systems, devices and services against malicious activities, and threats;
- logging and investigating network, applications, and user activities for the purpose of investigating faults, security breaches, and unlawful activity; and
- regularly auditing the security of information systems and reporting to appropriate University committees, including the Audit, Risk and Safety 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 is required. Cooperation and collaboration with law enforcement authorities may also be required.

4.8 Incident Notification and Response

1. Suspected Cyber Incidents must be promptly reported to cyber@bond.edu.au or the IT Service Desk.
2. Bond must maintain a cyber incident response capability supported by a documented incident response procedure. This procedure must clearly define roles and responsibilities and cover the following stages:

    - Preparation;
    - Discovery, validation and logging;
    - Identification;
    - Containment;
    - Eradication;
    - Recovery and root cause analysis; and
    - Learning and improvement.

3. The incident response procedure must be reviewed at least annually and updated as required.

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 or further disciplinary action. It may also be regarded as misconduct and dealt with under the Bond University Staff or Student Code of Conduct policies.

Depending on the breach, offenders may also be prosecuted under State, Commonwealth, and International laws.

6. DEFINITIONS, TERMS, ACRONYMS

Applications Custodians:	The key person nominated within Bond who is the point of contact for any issues or access to information within a system.
Cyber Incident / Incident:	An unwanted or unexpected cybersecurity event that has a significant probability of compromising business operations in any way. This includes the actual or potential unauthorised access, use, disclosure, disruption, modification, inspection, recording, or destruction of information.

Devices:	All computing hardware (including desktops, laptops, servers, virtual machines, IoT equipment, smartphones and tablets) accessing, developing, storing or processing university information assets.
Mobile Device Management (MDM):	Software that facilitates remote wiping, encryption and other hardware controls.
Personally Identifiable Information (PII):	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.
Privacy Impact Assessment (PIA):	Documented analysis of PII data storage to outline risks, impact and mitigation measures.
Software:	Software, for the purpose of this Policy includes: – Software installed on university assets and devices. – Software as a Service – Cloud based software subscriptions. – Free software – Software developed by or on behalf of Bond.
University Information Assets:	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.

7. AFFILIATED PROCEDURES AND SCHEDULES

ICT Acceptable Use Policy INF 6.1.11
IT Secure Development Guidelines
Data Breach Response Plan
Password Management Procedures
Information Protection Guidelines
Privacy Impact Assessment template
Information Security Policy Checklist

8. RELATED DOCUMENTS

Privacy Policy (INF 6.5.1)
Compulsory Training Policy (GOV 1.1.4)
Software and Software Subscriptions Policy (INF 6.1.6)
IT Account Termination Procedure
Student Code of Conduct Policy SS 5.8.2
Student General Misconduct Procedure
Staff Code of Conduct Policy(HR 2.8.4)

9. MODIFICATION HISTORY

Date	Sections	Source	Details
20 March 2025	All	Director ITS	V5: Rewrite to simplify and include additional security requirements introduced in 2024
13 July 2023	All	ITS	V 4.1 Update Contact Officer role and document links
19 May 2021	All	ITS	V4
29 November 2007			Date First Approved

APPROVAL AUTHORITY: Vice Chancellor

INF 6.5.3 Information Security Policy Checklist

Access and Storage

- ☐ Access to information is to be granted on a “least privilege” principle, be reviewed regularly and adjusted when contracts are terminated or roles change.
- ☐ Bond staff, students and Alumni must not divulge, copy, release, sell, loan, alter or destroy any Bond Information without appropriate authorisation.
- ☐ All users must report suspected breaches of data or systems immediately to cyber@bond.edu.au or the IT Service Desk.
- ☐ Multi-Factor Authentication is required for access to Bond University’s systems and data.
- ☐ Bond information must only be stored on Bond sanctioned storage and backed up on a regular basis.
- ☐ Non-Bond managed devices must not access, process, develop or store Bond Information. An MDM may be required if an exception is granted.
- ☐ Knowingly disclosing passwords or other access credentials will be deemed a breach of Policy.
- ☐ Bond network accounts are not to be used to register for personal software or other online services.
- ☐ Passwords used on all systems must comply with Bond’s Password Management Procedure
- ☐ Ensure appropriate approvals are granted before sharing information with people or organisations external to Bond or granting access within Bond.
- ☐ Staff IT accounts must be disabled on or before termination date.
- ☐ Information assets are to be disposed of securely.
- ☐ Retention and Disposal requirements must be adhered to.
- ☐ Data should be classified as per the Information Protection Guidelines
- ☐ All sensitive data should be encrypted.
- ☐ Personally identifiable information (PII) stored must be kept to a minimum. A Privacy Impact Assessment must be completed for systems that contain significant PII data.

Devices and software

- ☐ Any device connecting to or installed on a non-guest Bond network must be authorised by the Director, Information Technology Services or Chief Information Security Officer.
- ☐ Devices that are used to store or access Bond information, including accessing Bond email, must be securely configured as per ITS requirements.
- ☐ Devices that do not comply with security requirements will be removed from the network.
- ☐ Devices must be locked and securely stored when not in use, this including when working from home.
- ☐ Bond information assets are not to be stored on personal devices or within personal software subscriptions.
- ☐ Software development must comply with Software Develop Guidelines whether developed by staff or third parties on behalf of Bond.

☐ Software and subscriptions, regardless of cost, must be assessed and approved prior to purchase in accordance with the Software and Software Subscriptions Policy prior to use.

☐ Software must only be accessed if a licence or subscription has been granted.

☐ Software must be regularly updated to ensure security is maintained.

☐ Devices must be returned to ITS when a staff member leaves to ensure any data and permissions are wiped securely before reallocation or disposal.

☐ Software is to include advanced authorisation features such as Single Sign-on.

☐ Software and software updates must be tested thoroughly before being added to the production environment.

Other

☐ Staff must maintain awareness of the information security risks, guidelines, and controls appropriate to the information assets they access, create and use.

☐ Annual compulsory Cyber Security training must be completed by all staff and if applicable to the role Privacy Training should also be completed annually.

☐ Annual penetration testing will be completed.

☐ Activities may be monitored and recorded by ITS systems and staff. Bond reserves the right to access logs, audit trails and individual files. In carrying out these tasks, cooperation with the Information Security team is required.

☐ 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.

☐ Appropriate due diligence must be conducted on third parties that will process, store, host or have access to Bond information assets or sensitive systems. Contracts must be reviewed by ITS or General Council to ensure security and confidentiality clauses are appropriate.

☐ Any exemptions from this Policy must be approved by the VPO and Director ITS.

☐ 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 or further disciplinary action.