BOND UNIVERSITY	**IT ACCOUNT TERMINATION PROCEDURE**
Endorsing Policy	ICT Acceptable Use Policy
Procedure Owner	Director, Information Technology Services
Contact Officer	Director, Information Technology Services
Endorsement Authority	Vice President Operations
Date of Next Review	February 2028

1. PURPOSE AND OBJECTIVES

The purpose of this Procedure is to provide a framework that ensures the protection of Bond University's information assets and systems from unauthorised access, loss or damage and to comply with regulatory and legislative obligations by ensuring that IT Account access is removed when formal relationships between account holders and the University end.

2. AUDIENCE AND APPLICATION

All local and remote staff, Students, Alumni, and other Third Parties that have access to Bond's ICT systems.

3. ROLES AND RESPONSIBILITIES

Role	Responsibility
IT Account Holders	are expected to: ▪ Safeguard their IT account in accordance with the ICT Acceptable Use Policy and any other applicable University standard, procedure, guideline, or policy. ▪ Be aware of all legal and corporate responsibilities concerning inappropriate use, sharing or releasing of information from their IT accounts outside the Bond computer network. ▪ It is the responsibility of the departing individual to delete or transfer all files and email messages that are of a personal nature.
Application Custodians	are responsible for: ▪ Removing access to systems when user IT accounts are terminated. ▪ Modify system access where users change positions and access requirements change. ▪ Reviewing access on a periodic basis and must promptly revoke access no longer required by Users to ensure effective access control and prevent access creep. ○ All special or Privileged Access to systems (such as administrative or supervisor accounts) must be reviewed every six (6) months. ○ User access must be reviewed at regular intervals not exceeding twelve (12) months.
ITS	▪ Upon advice from P&T and other termination processes, ensure IT accounts are terminated in a timely manner and notify Application Custodians of terminations by sending an email to the usermanagement@bond.edu.au email distribution list, which contains contacts that have other system actions related to termination (i.e. Procurement, Security, FinanceOne, StudentOne, CRM, etc).
Staff /Third-party Bond supervisor	▪ Work with the departing individual to arrange for the preservation of all business-related files both from the individual's personal drives and email. ▪ Complete termination form for staff and email to P&T and confirm correct termination dates are entered into Bond's HR system to ensure the IT account is disabled. ▪ Ensure that ITS are notified of correct termination dates or changed dates for third-party users via the IT Service Desk (established when account created). ▪ Contact ITS if out of office email is required for terminated accounts. This can be established for a maximum of three months (as a licence is required). ▪ Ensure access changes as a result of position changes are actioned by the appropriate areas. ▪ Request VPO approval for any forwarding of email or access to personal drives such as OneDrive.
Chief People Officer or Deputy Director of People & Talent (P&T)	▪ Notify the Director of ITS **in advance** of pending involuntary terminations. ▪ Ensure staff terminations are actioned in a timely manner within the HR system to trigger termination of ITS account.

Student Services	▪ Ensure the status of students is maintained in the Student Management System which is used to manage the status of the IT account including termination actions.

4. PROCEDURE STATEMENT

4.1. Student Account Termination

Student

Early termination of student IT accounts is triggered from the Student Management System. On termination account contents are no longer available.

Outside of early termination, Students maintain IT account access until the conferral date of their award or until the date results are released for non-award programs (e.g. Student for a Semester and Study Abroad). Once these dates have passed, students are considered alumni, and the IT account is modified.

An Alumni alias is added to the existing student account and access to a small set of systems will be available, such as:

- iLearn courses for two (2) years post completion of the relevant course,
- Alumni systems,
- Adobe Express for six (6) months after graduation,
- Email.

Alumni

Bond provides continuity of email account access to Bond Alumni. Alumni have the opportunity to retain their email accounts for life or they can choose to provide alternative contact details to the Alumni office.

Alumni email accounts not utilised for a period of one (1) year will be disabled.

Learners

Learner accounts are managed through the Blackboard Learn platform. These accounts are considered lifelong accounts and are linked to an external email address.

Learner accounts may be made inactive after two (2) years of inactivity. Inactive accounts can be re-enabled by contacting the Executive Education unit.

4.2. Staff and Third-Party Account Termination

Staff or Third Party - Voluntary

IT accounts for an individual who voluntarily terminates employment with Bond University will be disabled on **the last day of employment** and content will no longer be available.

Staff or Third Party - Involuntary

For involuntary University-initiated terminations, network accounts will be disabled **immediately** and content will no longer be available.

Semesterly Staff Appointments

If a faculty member is not teaching consecutive semesters, their IT accounts will remain active until P&T request that the account is terminated.

4.3. Staff Change of Position

Upon notification of a staff member's reassignment to a new position, the ICT account is not terminated. However, access controls will need to be revoked or modified, including access to data stores, systems, and physical access to buildings for which they are no longer entitled and to grant access to that which they should.

4.4. Access to Data After Account Termination

All files stored on University equipment or storage are the **property of the University**, and that the University has no obligation to provide access to any files created and stored on University devices or storage.

All departing individuals and/or third parties will have, until their last day of employment, graduation or the last day of the applicable contract, access to their personal data on the Bond network, PC or cloud storage. They are not to remove or delete any data that is not their own, is necessary for the operation of the department or University, required by University retention policies, protected by law or placed under a litigation hold.

Where a person requests a copy of personal files, after termination, a request must be submitted to the IT Service Desk, including justification and Authorised Approval.

4.5. Extended Access to Account after Termination

No access is to be granted to the account once termination has been processed as per auditing requirements.

4.6. Suspension of Account

Bond University reserves the right to disable or terminate IT account access for any reason including security concerns, threats to ICT services, inappropriate use of ICT services, systems or software, or misconduct.

5. DEFINITIONS, TERMS, ACRONYMS

Alumni: Individuals that have successfully completed a Bond degree or certificate program.

Application Custodian: An individual or collective group with accountability and authority for University services or systems.

Authorised Approver: A person authorised to approve exceptions from this Procedure.

Faculty: Provost or Executive Dean of Faculty
HDR Students: Provost and Manager, HDR Unit
Staff or third party: Vice President Operations

In situations where the Authorised Approver listed above is unable to perform this duty in the manner or timeframe needed, their official delegate will assume decision authority.

IT Account: Account that provides access to University ICT services, systems and resources. This includes access to Network drives, SharePoint, Teams, Email, OneDrive, other systems.

Learner: A person registered and enrolled in a microcredential or executive education course via the Bond Learner Portal. A Learner is not an enrolled student.

Privileged Access: Access to elevated administrative roles within operating systems, databases, and applications – for example, back-end system configuration access.

Student: A person who is enrolled in one or more subjects or a research program offered by the University.

Third Party: An external individual engaged by the University to perform specific tasks or services without being a direct employee. This includes contractors, work experience appointments, and volunteers.

6. RELATED DOCUMENTS

ICT Acceptable Use Policy (INF 6.1.11)
Information Security Policy (INF 6.5.3)
Termination Procedure Checklist

7. MODIFICATION HISTORY

Date	Sections	Source	Details
11 February 2025	All	Director ITS	3-year cyclical review – revisions and simplification and convert to procedure
6 September 2021			Date First Approved

APPROVAL AUTHORITY: Vice Chancellor