BOND UNIVERSITY	**IT ACCOUNT TERMINATION POLICY**
Contact Officer	Director, Information Technology Services
Date First Approved	6 September 2021
Approval Authority	Director, Information Technology Services
Date of Next Review	6 September 2024

1. PURPOSE AND OBJECTIVES

The purpose of this Policy 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, executive, contractors and any other parties that rely on access to Bond's ICT systems.

This Policy applies to all University faculty and staff, Students, alumni and those third parties that have been provided an IT account to access Bond's ICT systems or services.

3. ROLES AND RESPONSIBILITIES

Role	Responsibility
All Bond University faculty, staff, students and others granted access to University systems via an IT account	are expected to: ▪ Safeguard their IT account in accordance with the Acceptable Use Policies and any other applicable University standard, procedure, guideline, or policy. ▪ Faculty/Office Managers of staff must ensure correct termination dates are entered into Bond's HR system for staff terminations to ensure the IT account is disabled in a timely manner. ▪ Faculty/Office Managers must ensure that correct termination dates are entered into Bond's HR system (or advised to IT Services) for third-party (e.g. contractor, consultant, volunteer, etc) terminations to ensure the IT account is disabled in a timely manner. ▪ Student Services are responsible for ensuring the status of students is up to date in the Student Management System. ▪ Departing individuals must return any allocated ICT equipment or other assets on, or prior to, departure from Bond. ▪ 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. ▪ If the Office of the General Counsel has placed a litigation hold on any student, staff or Third Party's data, it is prohibited to alter the contents of said data until the Office of the General Counsel lifts the litigation hold. ▪ As part of the termination process, the IT Service Desk sends an email to the usermanagement@bond.edu.au email distribution list, which contains contacts that have actions related to termination (i.e. Procurement, Security, FinanceOne, StudentOne, CRM, etc).
Staff member's Faculty/ Office Manager	Clause 4.5 Submit to IT Service Desk any requests that relate to the transfer of email or other processes that need to be migrated from the departing individual to a different individual in the department.
Director of HR	Clause 4.5 Must notify the Director of ITS **in advance** (where possible) of pending involuntary terminations.

4. POLICY STATEMENT

4.1. Student Account Termination

Accounts for students leaving the University for the following reasons are disabled immediately and deleted (all content) after 30 days:

- Absence without official leave for two (2) semesters or longer.
- Expulsion from the University (once the internal appeal process is finalised and the right to appeal has lapsed).
- Termination of Higher Degree Research candidature.
- Cancellation of enrolment (e.g. academic exclusion, unpaid fees, withdrawal from program or transfer to another institution).
- Student is deceased.

Outside of the exceptions above, student accounts maintain full access until the conferral date of their award or at least 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 will only retain access to email, iLearn courses for 2 years post completion of the relevant course, the alumni system, eStudent, and the "Scout" career system. Other data will be maintained for a period of 30 days after this date and will then be deleted.

Students in award programs are sent reminder notifications to their Bond email addresses prior to conferral to ensure that any data is backed up prior to the revocation of access.

4.2. Alumni E-mail Access

Bond provides continuity of email account access to Alumni. Alumni have the opportunity to retain their Student email accounts for life.

Alumni utilising Bond email services shall continue to comply with all applicable policies and controls when using their Bond email address.

Alumni emails not utilised for a period of one (1) year will be disabled, however can be re-enabled at a future date on individual request by the Office of Engagement to the IT Service Desk. Alumni will be required to register for multi-factor authentication.

Forwarding of emails outside of the Bond domain is not permitted and any forwarding rules should be removed by the student prior to graduation.

4.3. Learner Account Termination

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

Due to these accounts holding the Learner's course records, they will not be terminated unless there has been no activity on the account for fifty years.

Learner accounts may be made inactive after two years of inactivity. Inactive accounts can be re-enabled after a verification of identity through the user's associated external email.

If a Learner changes their external email address, they will be required to create a new account from the Bond Learner platform. If access to prior records is required, the Learner will need to contact the Microcredential Unit to make a request.

4.4. Staff Voluntary Termination

This includes network account terminations for voluntary staff-initiated separations (VEI), voluntary University-initiated separations (VUI), and Fixed Term contract expiration separations (FTC).

Network accounts for an individual who voluntarily terminates employment with Bond University will be disabled on **the last day of employment** and deleted (all content) after 90 days.

In all voluntary termination cases, the following procedures shall apply:

1. Upon notice of termination, the staff member's Faculty/Office Manager should work with the departing individual to arrange for the preservation of all business-related files both from the individual's network space and email.

2. It is the responsibility of the staff member's Faculty/Office Manager to submit to IT Service Desk any requests that relate to the transfer of email or other processes that need to be migrated from the departing individual to a different individual in the department, even if this is on a temporary basis.
3. It is the responsibility of the departing individual to delete or transfer all files and email messages that are of a personal nature and remove any email forwarding rules that may be in place prior to the last day of employment.
4. The Faculty/Office Manager may decide whether files are to be transferred to a designated location on the network, such as a shared departmental space, for example, or transferred to another individual.
5. An "auto-response" should be added by the departing individual to their mailbox (using the "Out of Office Assistant" tool in Outlook) on their last day of employment stating that the person is no longer in the employ of Bond University and indicating where future business messages should be sent. (Business emails are typically forwarded temporarily to the Faculty/Office Manager or another department co-worker.)

Individuals whose employment is ending but will remain actively enrolled as a student will be required to continue their student work with their Bond student account.

4.5. Staff Involuntary Termination

For involuntary University-initiated terminations, network accounts will be disabled **immediately** and deleted (all content) after 30 days.

In all cases of staff involuntary termination, the following procedures shall apply:

1. As part of the termination process, The Director of HR, or another authorised representative from the Vice President Operation's office, must notify the Director of ITS **in advance** (where possible) of the pending involuntary termination so that appropriate arrangements may be made for any transfer of files and timely closing of the IT account of the person to be terminated.
2. The Director of ITS will then arrange to revoke access, disable accounts, remove any email forwarding rules and secure all files on the staff member's network drive and mailbox.
3. If so desired, IT Services will arrange to transfer all files and email messages of the terminated staff member as part of the process of closing the account. These may be transferred to a designated network space or another individual with the Faculty/Office Manager's approval.
4. The Human Resources Office and/or the respective Department Head shall make certain that the designated person in IT Services is involved in the involuntary termination at the appropriate time.
5. The Department Head may decide whether files are to be transferred to a designated location on the network, such as a shared departmental space, for example, or transferred to another individual. At the discretion of the Authorised Office (refer Definitions), a copy of some or all these files may be given to the terminated staff member.
6. An "auto-response" will be added by IT Services to the terminating staff member's mailbox (using the "Out of Office Assistant" tool in Outlook) stating that the person is no longer in the employ of Bond University and indicating where future business messages should be sent.

4.6. Semester Appointments

If a faculty member is not teaching consecutive semesters, their IT accounts will remain active until they have had no employment service with the University for twelve (12) consecutive months or more. They will have full access to their Bond account during this time.

IT processes will automatically terminate the IT account once the termination date has been entered in the HR system for that staff member.

4.7. Inactive Casual Staff

If a casual staff member has had no employment service with the University for twelve (12) consecutive months or more, their IT account will terminate in accordance with this Policy for terminated staff members.

Casual Staff should be Terminated within the HR System by their Manager if they have no future dated assignments or have not had an active assignment for the past six (6) months. IT processes will then automatically terminate the IT account once the termination date has been entered in the HR system for that staff member.

4.8. Staff Change of Department

Upon notification of a staff member's reassignment to a new department, the Faculty/Office will notify administrators responsible for access controls, including ITS, Security, Finance or other applicable departments who will modify the staff member's/third party's access to Bond data, electronic systems, and physical access to buildings for which they are no longer entitled and to grant access to that which they should.

The change in ITS access may be to include a new drive or system and exclude an old drive or system. There is an existing IT form to complete for staff transfer between departments. This form should indicate whether the change is a permanent change (in which case old access permissions will be revoked, and new access permissions granted), or a secondment (in which case old access permissions will be temporarily revoked and new access permissions temporarily granted for the duration of the secondment), or an additional job (in which case new access permissions will be granted).

The Faculty/Office Manager of the staff member's former Faculty/Office will instruct the staff member to transfer all former department data to which they still have access. The staff member must transfer all data and/or email that is required to be retained by Bond retention policies or by law to the appropriate individuals.

4.9. Access Reviews

Asset Owners are responsible for reviewing system access and must:

1. Review access on a periodic basis and must promptly revoke all privileges no longer required by Authorised Users.
    a. All special or Privileged Access to systems (such as administrative or supervisor accounts) must be reviewed every six (6) months.

b. All Authorised User access must be reviewed at regular intervals not exceeding twelve (12) months including when they change roles, in order to maintain effective access control and to prevent access creep.

4.10. Access to Data After Account Termination

Terminating individuals and graduating students must remember that all files stored on University equipment or storage are the **property of the University**, and that the University has no obligation to provide them with access to any files created and stored by them 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 third-party contract, access to remove or copy personal data from Bond systems to their personal 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.

In cases where a departing person requests a copy of files from a Bond network, PC or cloud storage drive, or access to their email account to retrieve "personal" information after termination, this is **not permitted**. While Bond University understands and allows reasonable personal use of its email system, users should take appropriate steps to ensure personal communications are secured/saved as desired prior to termination.

Faculty/Office Managers can request access to the terminated staff member's files after the Account has been terminated, with approval from the Vice President, Operations (VPO). A request should be submitted to the IT Service Desk, including business justification and VPO approval.

4.11. Extended Access to Account after Termination

If it is necessary that an individual maintain access to their IT account beyond their termination date ("Extension of Access"), approval must first be secured from the Authorised Official identified (refer Definitions within this Policy).

Extension of access should be considered only if a legitimate business need is identified. Extension of use should not exceed one (1) month. In such cases, the individual will still be expected to adhere to Bond's Acceptable Use and other relevant policies and procedures.

In all cases, no person may retain a copy of any private or confidential work-related email or electronically stored information after the termination of employment without the written permission of the Authorised Official within this Policy.

4.12. Suspension of Account

Bond University reserves the right to 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

Account:	A username or other identifier which, with or without a password, allows a user to access University ICT services or systems.
Alumni:	Individuals that have successfully completed a Bond degree or certificate program.
Asset Owner:	An individual or collective group with accountability and authority for University ICT services or systems.
Authorised Official:	A person authorised to approve extended IT account access beyond termination. 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 Official listed above is unable to perform this duty in the manner or timeframe needed, their official delegated authority will assume decision authority.
Learner:	A person registered and enrolled in a microcredential course on the Bond Learner Portal. A Learner is not entitled to or allowed access to any Bond University facilities unless they are enrolled as a Student.
Privileged Access:	Access to 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 individual that is not directly employed by the University or not an enrolled student. This includes contractors, work experience appointments, and volunteers.

6. RELATED DOCUMENTS

Staff Acceptable Use of ICT Facilities Policy
Student Acceptable Use of ICT Facilities Policy
Privacy Policy
Information Security Policy

7. MODIFICATION HISTORY

Date	Sections	Source	Details