Apprenticeships Are Us

IT ACCESS CONTROL POLICY

PURPOSE

The purpose of this policy is to establish a consistent and secure framework for managing user access to Apprenticeships Are Us Ltd (ARU) information systems, networks, and data.

It aims to:

- Protect the confidentiality, integrity, and availability of ARU's information assets.
- Prevent unauthorised access, data loss, or misuse of systems.
- Ensure compliance with applicable legislation and recognised standards, including:
    i. Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).
    ii. Fair Work (Registered Organisations) Act 2009 – protection of employment records.
    iii. Cyber Security Act 2018 and the Australian Cyber Security Centre (ACSC) Essential 8 Maturity Model.
    iv. ISO/IEC 27001:2022 Information Security Management Systems.
    v. National Standards for Group Training Organisations (2017).

SCOPE

This policy applies to:

- All employees, contractors, board members, apprentices, and third-party vendors who access ARU's systems, networks, or data.
- All IT systems, including but not limited to:
    i. MYOB AccountRight / Advanced (financial).
    ii. Workforce One (GTO and HR management).
    iii. Microsoft 365 and SharePoint (document management and email).
    iv. Power BI (dashboards and reporting).
    v. BoardEffect (board governance portal); and
    vi. Any other cloud-based or locally hosted applications containing corporate information.

The policy applies equally to on-premises, cloud, and remote-access environments.

DEFINITIONS

Term	Definition
Access Control	The process of granting, restricting, and monitoring rights to systems or data.
Least Privilege	Granting the minimum level of access required to perform job duties.
Role-Based Access Control (RBAC)	A model assigning access rights based on defined organisational roles.
Deprovisioning	Revoking system access promptly when a user leaves ARU or changes role.
Information Asset	Any data, record, or digital resource owned or managed by ARU.

POLICY PRINCIPLES

1. Least Privilege Principle

Each user will be granted only the access necessary to perform their designated role. Elevated or administrative privileges must be justified in writing and approved by the Managing Director (MD).

2. Role-Based Access

Access rights will align with the Role-Based Access Matrix (RBAM) approved by the Operations Manager. All systems must enforce role-based permissions consistent with that matrix.

3. Segregation of Duties

Responsibilities shall be divided to prevent conflicts of interest or fraud (for example, the person processing payroll cannot authorise payments).

4. Formal Approval

All provisioning, modification, and removal of access must follow documented approval workflows using ARU's Access Request Form or Helpdesk Ticketing System.

5. Timely Deprovisioning

Access for departing or transitioning staff must be revoked within one business day of employment termination or role change, in accordance with HR notification protocols.

6. Audit Trail

All access changes must be logged and retained for a minimum of two years. Audit logs must be reviewed quarterly by IT Administration and independently verified by the Financial Controller.

PROCEDURES

1. Access Request

1. The employee's line manager completes an Access Request Form, specifying required systems and permissions.
2. The Operations Manager verifies alignment with the RBAM and approves provisioning.
3. IT Administration implements access and records the change in the Access Register.

2. Modification of Access

1. Any role change or additional access requires re-approval from the line manager and MD.
2. Access modification logs must be updated and retained for audit purposes.

3. Deprovisioning of Access

1. Upon employee resignation, termination, or contract completion, HR notifies IT within 24 hours.
2. IT disables all system accounts and retrieves or reassigns devices and credentials.
3. The deprovisioning process is verified by the Operations Manager and signed off by HR.

4. Periodic Access Review

- Quarterly reviews are conducted by IT Administration to confirm that active accounts remain appropriate.
- Reviews include comparison against the HR roster and contractor register.
- Findings are reported to the MD and summarised in the Continuous Improvement Committee minutes.

5. Access Monitoring and Logging

- All system access logs, authentication attempts, and administrative changes must be captured and stored securely.
- Alerts are configured for multiple failed login attempts, privilege escalations, or unauthorised access.

6. Incident Reporting

- Any suspected breach, misuse, or unauthorised access must be reported immediately to the Operations Manager and logged in the WHS & Risk Register.
- Incidents involving potential data exposure are escalated to the MD and may require reporting to the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breaches Scheme (Part IIIC of the Privacy Act 1988).

7. Password and Authentication Standards

- All accounts must use multi-factor authentication (MFA) where supported.
- Passwords must meet ARU's Password Policy (minimum 12 characters, mix of cases and symbols, renewal every 90 days).
- Generic or shared accounts are prohibited.

COMPLIANCE AND AUDIT

- Compliance with this policy will be tested annually as part of the Internal Controls Audit and external audit by Apprenticeships Are Us Ltd nominated auditors during the applicable financial year.
- Evidence of access reviews, deprovisioning logs, and exception reports must be retained.
- Non-compliance or control weaknesses will be documented in the Corrective Action Register and reviewed by the Continuous Improvement Committee.

TRAINING AND AWARENESS

- All staff and contractors receive induction training on cybersecurity and acceptable-use obligations.
- Refresher sessions are conducted annually and whenever systems or policies change.
- Awareness materials (posters, intranet articles) reinforce best practice and ARU's security culture.

ENFORCEMENT

Failure to comply with this policy may result in:

- Revocation of system access.
- Formal disciplinary action, up to and including termination of employment.
- Referral to law-enforcement or regulatory authorities where legislation has been breached.

REFERENCES

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs) 12 & 13
- Cyber Security Act 2018 (Cth)
- ISO/IEC 27001 and 27002 (Access Control Annex A 5 & 8)

- ACSC Essential 8 Controls – User Application Hardening & Access Management
- National Standards for Group Training Organisations (2017
- ARU Role-Based Access Matrix (RBAM)
- ARU Information Security Policy
- ARU Business Continuity and Disaster Recovery Framework

DOCUMENT CONTROL

Version	Authorised by	Authorisation Date	Change Summary
1.0	ARU Board of Directors	01/07/2025	Initial release – aligned to ISO/IEC 27001:2022, Privacy Act, Cyber Security Act, ACSC Essential Eight, National Standards for GTOs