Apprenticeships Are Us

ROLE-BASED ACCESS MATRIX (RBAM)

PURPOSE

The Role-Based Access Matrix (RBAM) defines and governs the allocation of system access permissions across all positions within Apprenticeships Are Us Ltd (ARU).

Its purpose is to:

- Ensure that access to systems and data is granted on the principle of least privilege, meaning users only have access required to perform their duties.
- Enforce segregation of duties (SoD) to mitigate the risk of error or fraud.
- Establish transparent approval workflows for the provisioning, modification, and deprovisioning of access.
- Support compliance with:
    i. **ISO/IEC 27001:2022** – Annex A.9 (*Access Control*).
    ii. **Privacy Act 1988 (Cth)** – Australian Privacy Principles (APPs 6–13).
    iii. **Cyber Security Act 2018 (Cth)**; and
    iv. **National Standards for Group Training Organisations (2017)** – Standard 4 (*Governance and Risk Management*).

SCOPE

This matrix applies to:

- All ARU employees, contractors, and consultants who access ARU's systems and networks.
- All business systems, cloud applications, and data repositories including:
    i. **MYOB** (finance and payroll)
    ii. **Workforce One** (apprentice management and HR)
    iii. **Power BI** (financial and operational dashboards)
    iv. **Microsoft 365 and SharePoint** (communications, file storage, governance)
    v. **BoardEffect** (board papers and policy management)

The matrix must be applied consistently across all states and operational divisions of ARU.

ACCESS MANAGEMENT PRINCIPLES

1. **Role-Based Access:**
   Access rights are granted according to a user's position and responsibilities as defined below.
2. **Approval Workflow:**
   All access requests must be approved by the designated approver before implementation.
3. **Auditability:**
   Each access assignment or change must be documented, time-stamped, and filed.

4. **Periodic Review:**
   The General Manager conducts quarterly reviews of all access permissions against the current organisational chart.

5. **Deprovisioning:**
   Access is revoked within one business day of termination, transfer, or contract expiry.

6. **Confidentiality:**
   Users are required to sign the ARU Confidentiality and Data Protection Agreement prior to gaining system access.

ROLE DEFINITIONS AND ACCESS PERMISSIONS

Role	System Access	Access Type	Approval Level	Notes / Restrictions
Managing Director (MD)	MYOB, Workforce One, Power BI, SharePoint, BoardEffect	Full Administrator	Board Chair	Access to all systems for oversight and strategic management. Excluded from direct payroll entry or modification of employee pay categories to maintain segregation of duties.
Finance Manager	MYOB, Power BI	Read/Write	Managing Director	Full finance access including journal entries, accounts receivable/payable, and reporting. Requires dual sign-off for payments and cannot authorise their own expense claims.
Payroll Officer	Workforce One	Read/Write	Finance Manager	Processes wages, superannuation, and entitlements. May not alter pay categories, awards, or base rates without written approval from the Finance Manager.
General Manager	Workforce One, Power BI, Microsoft 365	Read/Write	Managing Director	Oversees operational reporting and access management. Responsible for quarterly AEM access reviews and system integrity verification.
Apprentice Employment Managers (AEMs)	Workforce One	Read-Only (Regional Access)	General Manager	Restricted to their assigned regional portfolios. No access to payroll or finance data.
HR Coordinator	SharePoint HR Folder, Workforce One	Read/Write	Managing Director	Access is limited to HR and employee-related records. No access to financial documents or payroll. Ensures compliance with APP 11 (Data Security).
IT Administrator	All systems (technical layer only)	Administrator (Technical)	Managing Director	Responsible for system configuration, maintenance, and user provisioning. Cannot access or alter financial, payroll, or apprentice personal data. Must maintain SOC2-aligned logging and security controls.
External Auditor	MYOB, Power BI (Read-Only)	Temporary Access	Managing Director	Granted restricted access for financial audit purposes only. Access is revoked immediately following audit completion and verified via access log review.

ACCESS APPROVAL WORKFLOW

Access Activity	Initiated By	Approved By	Implemented By	Logged In
New User Access	Line Manager	General Manager	IT Administrator	Access Register
Access Modification	Employee / Manager	Managing Director	IT Administrator	Access Register
Role Transfer	HR	General Manager	IT Administrator	Access Register
Deprovisioning	HR	General Manager	IT Administrator	Access Register
External Auditor Access	Finance Manager	Managing Director	IT Administrator	Access Register

All access forms and approvals are to be stored electronically in Sharepoint.

MONITORING AND REVIEW

- **Quarterly Audits:** The Operations Manager reviews the Access Register quarterly to ensure compliance with the matrix and documents outcomes in the Continuous Improvement Committee (CIC) minutes.
- **Annual Audit:** Internal or external auditors (e.g. HLB Mann Judd) may test access controls, user permissions, and segregation of duties as part of the annual audit.
- **Exception Handling:** Any deviation or temporary elevation of privileges must be time-bound, documented, and approved by the MD.

LEGISLATIVE AND STANDARDS REFERENCES

- **Privacy Act 1988 (Cth)** – APP 6 (Use and Disclosure), APP 11 (Security of Personal Information)
- **Cyber Security Act 2018 (Cth)**
- **ISO/IEC 27001:2022** – Annex A.9 Access Control
- **Australian Cyber Security Centre (ACSC)** – Essential Eight: Access Control & Application Hardening
- **National Standards for Group Training Organisations (2017)**
- **ARU IT Access Control Policy** (cross-referenced)

ENFORCEMENT

- Breach of this matrix, unauthorised access, or failure to comply with approval workflows constitutes a breach of ARU's IT Access Control Policy and Code of Conduct.
- Disciplinary actions may include revocation of access, written warning, termination of employment, or escalation to relevant authorities under the Privacy Act 1988 (Cth).

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 & ARU IT Access Policy