Apprenticeships
Are Us

CYBER SECURITY POLICY

TABLE OF CONTENTS

INTRODUCTION 3

LEGISLATIVE, REGULATORY AND STANDARDS FRAMEWORK 3

Legislation 3

Cybersecurity Standards & Frameworks 3

Sector Standards 4

Internal Instruments 4

PURPOSE 4

DEFINITIONS 5

POLICY 5

RESPONSIBILITIES 7

PROCESSES 7

1. Monitoring 7

Cyber Risk Register 7

2. Confidentiality 8

3. System taxonomy 8

4. Data taxonomy 9

Multi-Factor Authentication (MFA) 9

5. Access control 9

Secure Configuration Management 10

Party & Vendor Cybersecurity Obligations 10

6. Computer security 10

Patch Management Requirements 13

7. Data Breach Response Plan 13

Cyber Incident Escalation & Governance 13

8. Optional 14

Business Continuity & Disaster Recovery 14

RELATED DOCUMENTS 15

AUTHORISATION 15

INTRODUCTION

As a registered Group Training Organisation (GTO), *Apprenticeships Are Us Ltd* adheres to the *National Standards for Group Training Organisations*, which require strong cybersecurity protocols to protect personal data and ensure the integrity of the systems that manage apprentice and trainee information. This policy ensures compliance with *National Standard 3 – Risk Management* by safeguarding against cyber threats and breaches that could compromise the operations of the organisation.

While Apprenticeships Are Us Limited (ARU) wishes to foster a culture of openness, trust, and integrity, this can only be achieved if external threats to the integrity of the organisation's systems are controlled, and the organisation is protected against the damaging actions of others.

In today's dynamic and interconnected digital landscape, the role of cyber security cannot be overstated. The emergence of sophisticated threats and vulnerabilities in the realm of information technology necessitates that organisation, including ARU, adopt robust cyber security policies. This section elucidates the compelling need and the significant benefits of maintaining strong cyber security policies within our organisation.

ARU aspires to cultivate a corporate environment characterised by transparency, confidence, and ethical conduct. However, the realisation of this vision hinges upon our ability to effectively manage external threats that may compromise the integrity of our organisational systems and safeguard the entity against potentially deleterious actions perpetrated by external factors.

LEGISLATIVE, REGULATORY AND STANDARDS FRAMEWORK

This Cyber Security Policy is governed by the following legislation, standards and frameworks:

Legislation

- *Cybersecurity Standards Act 2023 (Cth)*
- *Privacy Act 1988 (Cth)* and the Notifiable Data Breaches (NDB) Scheme
- *Corporations Act 2001 (Cth)* – directors' duties regarding asset protection
- *Australian Charities and Not-for-profits Commission Act 2012 (Cth)*
- *Fair Work Act 2009 (Cth)* – employee obligations for confidentiality and compliance
- *State and Territory WHS Acts and Regulations*

Cybersecurity Standards & Frameworks

- *ACSC Essential Eight Maturity Model*
- *Australian Government Information Security Manual* (ISM)
- *ISO/IEC 27001:2022 Information Security Management Systems*
- *ASD Hardening Guides*

Sector Standards

- National Standards for Group Training Organisations (2017), particularly Standard 3 – Risk Management
- Smart & Skilled contractual requirements
- ACNC Governance Standards 1, 2, 5 & 6

Internal Instruments

- ARU Code of Conduct
- ARU Privacy Policy
- ARU Data Breach Response Plan
- ARU Records Management Policy
- ARU Risk Management Framework
- ARU Acceptable Use of Electronic Media Policy

Directors are required to exercise due diligence under WHS law, privacy law and the Corporations Act to ensure ARU's cybersecurity systems are appropriate, functioning and regularly reviewed.

PURPOSE

As a registered charity under the *Australian Charities and Not-for-profits Commission (ACNC)*, ARU must comply with the *ACNC Governance Standards*. These standards require transparency and accountability in protecting personal data and maintaining cybersecurity protocols to safeguard information about employees, apprentices, and stakeholders. The implementation of this cybersecurity policy reflects ARU's commitment to upholding these governance standards.

This policy sets out guidelines for generating, implementing, and maintaining practices that protects Apprenticeships Are Us Limited's cyber media – its computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

This policy applies to employees, apprentices, contractors, consultants, and volunteers at ARU, including all personnel affiliated with third parties, to all equipment owned or leased by ARU, and to all equipment authorised by ARU for the conduct of the organisation's business.

This policy outlines the principles for developing, implementing, and upholding practices aimed at safeguarding the cyber assets of ARU, encompassing computer equipment, software, operating systems, storage media, electronic data, and network accounts, against potential misuse or exploitation. It is imperative that these guidelines adhere to the Privacy Act.

This policy extends its applicability to all personnel associated with ARU, encompassing employees, apprentices, contractors, consultants, volunteers, and third-party affiliates, as well as all equipment either owned or leased by ARU and equipment duly authorised by ARU for organisational purposes.

DEFINITIONS

Cyber Incident – Any attempt to gain unauthorised access, disrupt systems, steal data, or compromise confidentiality, integrity or availability.

Malware – Malicious software including viruses, ransomware, spyware, trojans or worms.

Phishing – Fraudulent attempts to obtain sensitive information by impersonating legitimate entities.

Multi-Factor Authentication (MFA) – A security system requiring two or more verification methods.

Privileged Access – Elevated system access that allows configuration or system-level changes.

Vulnerability – A weakness in software, systems or processes that may be exploited.

Critical Data – Any data classified as RED in ARU’s data taxonomy.

Personal Information – Data about an identified or reasonably identifiable individual under the Privacy Act.

POLICY

This policy complies with the *Corporations Act 2001 (Cth)*, which outlines the responsibilities of directors and officers to ensure proper governance, risk management, and the protection of corporate assets, including information systems. Ensuring cybersecurity is part of ARU's obligation to safeguard the organisation's assets and comply with corporate governance standards.

While Apprenticeships Are Us Limited wishes to provide a reasonable level of personal privacy, users should be aware that the data they create on the organisation’s systems remains the property of ARU. Because of the need to protect ARUs network, the confidentiality of information stored on any network device belonging to ARU cannot be guaranteed, and ARU reserves the right to audit networks and systems periodically to ensure compliance with this policy.

Information in the possession of the organisation shall be classified into different grades depending on its degree of confidentiality. Particularly sensitive information will receive special protection.

Employees, the ARU Board and volunteers will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.

Breach of this policy by any employee may result in disciplinary action, up to and including dismissal.

While ARU is committed to preserving a reasonable degree of personal privacy, it is essential for users to acknowledge that data generated on ARU’s systems remains the exclusive property of ARU. In light of the imperative need to safeguard ARU’s network, confidentiality of information residing on any network device owned by ARU cannot be unconditionally guaranteed, and ARU retains the prerogative to periodically conduct audits of networks and systems to ensure compliance with this policy.

Information held by the organisation will be categorised based on its level of sensitivity, with particularly confidential data receiving heightened protective measures.

Employees, ARU Board members, and volunteers are obligated to rigorously adhere to established cybersecurity procedures, including the secure management of passwords, the protection of computer access, and the maintenance of protective software.

Failure to adhere to this policy by any employee may result in disciplinary action, which could extend to dismissal.

The Need for Strong Cyber Security Policies:

1. **Protection of Sensitive Data**: Cyber security policies are indispensable for safeguarding sensitive information, such as personal and financial data of our apprentices, employees, and partners. The potential fallout from data breaches, including legal repercussions, reputational damage, and financial loss, underscores the urgency of protecting this data.
2. **Mitigation of Cyber Threats**: As technology advances, so do the capabilities of malicious actors. Robust policies help ARU identify, manage, and mitigate cyber threats, ensuring that the organisation remains resilient against evolving attacks, including malware, phishing, and ransomware.
3. **Legal and Regulatory Compliance**: In today's regulatory landscape, adherence to cyber security standards is not just advisable but often mandatory. Failure to comply with regulations, such as data protection laws, can result in severe penalties. A well-defined cyber security policy ensures ARU's compliance with relevant legal and regulatory requirements. This policy ensures ARU's compliance with all applicable Australian legislation and standards, including but not limited to:
    - *Privacy Act 1988* (Cth)
    - *Cybersecurity Principles* outlined by the Australian Cyber Security Centre (ACSC)
    - *Corporations Act 2001 (Cth)*
    - *ACNC Governance Standards* This compliance framework ensures that ARU adheres to its legal obligations while protecting its information assets.
4. **Preserving Business Continuity**: Cyber-attacks and security breaches can disrupt business operations, leading to costly downtime. Strong cyber security policies are instrumental in maintaining business continuity, reducing the risk of operational disruptions.

The Benefits of Strong Cyber Security Policies:

1. **Risk Reduction**: By implementing comprehensive cyber security policies, ARU mitigates risks associated with cyber threats and data breaches. This proactive approach helps protect the organisation's assets and reputation.
2. **Enhanced Trust and Reputation**: Strong cyber security policies build trust among apprentices, employees, partners, and stakeholders. Demonstrating a commitment to data protection enhances ARU's reputation and instils confidence in the organisation.
3. **Cost Savings**: Prevention is more cost-effective than dealing with the aftermath of a cyber incident. A robust cyber security policy can lead to substantial cost savings by reducing the likelihood of security breaches and their associated expenses.

4. **Improved Operational Efficiency**: Effective cyber security policies can streamline IT operations and ensure that resources are allocated efficiently. This, in turn, leads to improved overall operational efficiency within the organisation.

RESPONSIBILITIES

It is the responsibility of the Managing Director (MD) to ensure that:

- staff are aware of this policy;
- any breaches of this policy coming to the attention of management are dealt with appropriately;
- a cyber security officer is appointed.

It is the responsibility of the cyber security officer (Empower IT) to ensure that:

- the MD is kept aware of any changes to the organisation's cyber security requirements;
- a report on the organisation's cyber security is submitted annually to the board at the AGM.
- The cybersecurity officer (Empower IT) is responsible for ensuring that ARU remains compliant with both internal and external cybersecurity standards. Additionally, the officer will submit an annual cybersecurity report to the ARU Board at the AGM, including a detailed risk assessment of potential threats and an overview of the organisation's cybersecurity performance, in compliance with GTO National Standards, ACNC Governance Standards, and the *Corporations Act 2001 (Cth)*.

It is the responsibility of all employees and volunteers to ensure that:

- they familiarise themselves with cyber security policy and procedures;
- their usage of cyber media conforms to this policy.

In the event of any uncertainty or ambiguity as to the requirements of the cyber security policies or procedures in any instance, employees and volunteers should consult their supervisor.

PROCESSES

1. Monitoring

MD may authorise individuals with responsibility for cyber security issues in the organisation, including the cyber security officer (Empower IT), to monitor the organisation's equipment, systems and network traffic at any time for security and network maintenance purposes.

Cyber Risk Register

ARU maintains a dedicated Cyber Risk Register as part of the organisational Risk Management Framework.
It includes:

- identified cyber risks
- risk ratings
- mitigations

- treatment plans
- monitoring actions
- responsible officers

The Register must be updated quarterly and reviewed by the Board.

2. Confidentiality

Following consultation with the cyber security officer, the MD shall from time-to-time issue cyber security procedures appropriate to different levels of confidentiality.

The organisation shall classify the information it controls in the organisation's computer system files and databases as either non-confidential (open to public access) or confidential (in one or many categories).

The cyber security officer is required to review and approve the classification of the information and determine the appropriate level of security that will best protect it.

This policy ensures compliance with the *Privacy Act 1988*, which governs the handling of personal and sensitive information. ARU is committed to protecting the privacy of individuals by ensuring that confidential data, including apprentices' and employees' personal information, is stored and accessed securely. Any breach of data privacy will be handled in accordance with the *Notifiable Data Breaches (NDB) scheme* under the *Privacy Act*.

3. System taxonomy

Security level	Description	Example
Red	This system contains confidential information – information that cannot be revealed to personnel outside the company. Even within the company, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life-threatening consequences and/or an adverse financial impact on the business of the company.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information
Green	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access server and application(s). Management workstations used by systems and network administrators.
White	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
Black	This system is externally accessible. It is isolated from RED and GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public web server with non-sensitive information.

4. Data taxonomy

Security level	Description	Example
Red	Host Business data allowing financial exploitation or identity theft Organisation data allowing banking or financial exploitation	Host Business credit card and banking data Organisational credit card and banking data Host Business details that would facilitate phishing
Green	Host Business data allowing address or email exploitation Organisational intellectual property that has financial or reputational consequences	Addresses that would facilitate spamming Information that the organisation sells Internal emails
Black	Publicly accessible data	Non-sensitive information

Data and systems that contain sensitive information related to apprentices and trainees, as managed by ARU, must adhere to *National Standard 3 – Risk Management* for GTOs. This includes identifying and classifying systems and data based on their risk level and ensuring the appropriate security controls are in place for high-risk (RED) systems and data.

Multi-Factor Authentication (MFA)

MFA is mandatory for:

- email accounts
- remote access
- all administrative accounts
- access to sensitive systems (RED systems)
- any cloud-based application

MFA must use at least:

- authenticator app,
- token, or
- biometric verification.

SMS MFA may be used only as backup.

5. Access control

Individuals will be granted clearance levels for specific access to the organisation's information resources, and they are required to access only those resources for which they possess authorised clearance. Access control shall be administered through the implementation of username and password controls.

Secure Configuration Management

ARU systems must be configured according to industry-standard hardening guidelines (ACSC, CIS Benchmarks). This includes:

- disabling unnecessary services;
- enforcing strong encryption (TLS 1.2+);
- automatic OS and application updates;
- removing default admin accounts;
- enforcing screen lock and inactivity timeout.

Configuration drift must be monitored and corrected.

Party & Vendor Cybersecurity Obligations

All external vendors, contractors and service providers (including Empower IT) must:

- meet ARU's cybersecurity requirements
- maintain up-to-date certifications or attestations
- notify ARU of incidents affecting ARU systems
- implement MFA, encryption, patching and secure configuration
- maintain cyber insurance

Vendor access must be:

- limited;
- logged;
- time-restricted;
- regularly reviewed.

6. Computer security

6.1 All PCs, laptops and workstations should be secured by a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

6.2 Users must keep passwords secure. Accounts must not be shared, and no other people may be permitted to use the account. Passwords should not be readily accessible in the area of the computer concerned. Authorised users are responsible for the security of their passwords and accounts.

6.3 System level passwords should be changed quarterly; user level passwords should be changed every six months. User accounts will be frozen after three failed log-on attempts. Log-on IDs and passwords shall be suspended after 30 days without use.

6.4 Users who forget their password must call **Empower IT** on (02) 8030 8900 to get a new password assigned to their account. The user must identify themselves by [e.g., employee number] to [the IT department].

6.5 Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorised users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

6.6 Users will not be allowed to log-on as system administrators. Users who need this level of access to production systems must request a special access account as outlined elsewhere in this document.

6.7 Employee log-on IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the organisation. Supervisors/managers shall immediately and directly contact the IT manager to report change in employee status that require terminating or modifying employee log-on access privileges.

6.8 Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the company and require the permission of the organisation's cyber security officer. Monitoring of the special access accounts shall be undertaken via the periodic generating of reports to the cyber security officer showing who currently has a special access account, for what reason, and when it will expire. Special accounts will expire in 30 days and will not be automatically renewed without written permission.

6.9 All computers and devices used by the employees that are connected to the Apprenticeships Are Us Ltd.'s IT systems and software must be owned Apprenticeships Are Us Ltd and shall be continually executing virus-scanning software with a current virus database approved by the cyber security officer. IT hardware that is not owned by Apprenticeships Are Us Ltd is not authorised for use to access Apprenticeships Are Us Ltd.'s IT systems and software.

6.10 Malware protection software must not be disabled or bypassed, nor the settings adjusted to reduce their effectiveness.

6.11 Automatic daily updating of the malware protection software and its data files must be enabled.

6.12 All email attachments must be scanned. All documents imported into the computer system must be scanned. Weekly scanning of all computers should be enabled.

6.13 A record of the antivirus and anti-malware software should be kept.

6.14 Desktop computers in areas of public access should be physically secured by cables and padlocks.

6.15 Where possible, sensitive data should not be removed from the organisation's premises without specific authorisation.

6.16 Where this is not feasible, data on laptops that may leave the organisation's premises should be protected by full disk encryption.

6.17 Alternatively, staff who need access to sensitive data offsite should be given remote access privileges subject to adequate safeguards.

6.18 Computers being deaccessioned (whether for sale, reuse or disposal) shall not be released until all data has been securely deleted.

6.19 Users shall not download unauthorised software from the internet onto their PCs or workstations.

6.20 Users must use extreme caution when opening email attachments received from unknown senders; these may contain viruses, malware or Trojan horse code.

6.21 Users who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their [organisation designee] immediately. The user shall not turn off the computer or delete suspicious files.

6.22 Users must not themselves breach security or disrupt network communication on the organisation's systems or elsewhere. Security breaches include accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access unless these duties are within the scope of regular duties. "Disruption" includes network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

6.23 Users shall not attach unauthorised devices to their computers unless they have received specific authorisation from their manager or the company IT designee.

ARU prohibits the use of TOR or any anonymity-based browser.

Only the following secure browsers are permitted:

- Microsoft Edge (current version)
- Google Chrome (current version)
- Mozilla Firefox ESR (current version)

All browsers must:

- have automatic updates enabled;
- use ARU-approved security extensions;
- block third-party cookies;
- enforce HTTPS connections.

TOR is banned because it:

- bypasses monitoring;
- increases malware risk;
- creates audit gaps;
- increases exposure to malicious infrastructure.

6.24 Apprenticeships Are Us Ltd uses the services of Bit Fender for its Cyber Security Protection.

6.25 All IT assets and equipment used by ARU personnel, including laptops, desktops, and mobile devices, must adhere to the organisation's cybersecurity policies and procedures. Any device connecting to ARU's network must meet the minimum-security standards set by the cybersecurity officer (Empower IT), including the use of antivirus, encryption, and password-protected systems. All access to ARU’s data and network infrastructure must be in line with these security protocols.

ARU adopts the ACSC Essential Eight as baseline cybersecurity controls:

1. Application Control
2. Patch Applications (within 48 hours for critical patches)
3. Configure Microsoft Office Macro Settings
4. User Application Hardening
5. Restrict Administrative Privileges
6. Patch Operating Systems
7. Multi-Factor Authentication (MFA)
8. Daily Backups

ARU targets Maturity Level 2 and progressively increases maturity as resources allow.

Patch Management Requirements

All systems must:

- install security patches within 48 hours for critical vulnerabilities;
- install other patches within 14 days;
- maintain up-to-date versions of all software;
- remove unsupported or legacy software.

Empower IT must document patch cycles monthly.

7. Data Breach Response Plan

In the event of a data breach or cybersecurity incident, ARU will immediately activate its Data Breach Response Plan, which includes the following steps:

1. Identifying and containing the breach to prevent further damage.
2. Notifying relevant stakeholders, including the ARU Board, cybersecurity officer, and affected parties.
3. Assessing the scope and impact of the breach, including the type of information compromised.
4. Complying with reporting obligations under the *Notifiable Data Breaches (NDB) scheme* of the *Privacy Act 1988*.
5. Implementing measures to rectify vulnerabilities and prevent future incidents.

Cyber Incident Escalation & Governance

All cyber incidents must be escalated according to severity:

Critical Incidents (Immediate)

- ransomware;
- data exfiltration;
- system compromise;
- phishing attacks affecting staff;
- unauthorised privileged access;
- suspected criminal activity.

Must be reported to:

- Managing Director
- Cybersecurity Officer
- ARU Board (Chair)
- ACNC (where required)
- OAIC (if privacy breach)
- Police or ACSC if criminal or national-security risk

Moderate Incidents

- attempted but unsuccessful attacks;
- suspicious system behaviour;
- outages that affect operations.

Reported within 24 hours.

Minor Incidents

Logged in the cyber incident register and reviewed monthly.

8. Optional

Only devices that have received explicit authorisation may be connected to the organisation's network(s). Authorised devices encompass company-owned PCs and workstations that adhere to the company's configuration guidelines. Additionally, network infrastructure devices employed for network management and monitoring are also considered authorised.

Users are strictly prohibited from attaching non-company computers to the network that are neither authorised nor under the ownership or control of the company. Furthermore, users are prohibited from connecting any unauthorised storage devices, such as thumb drives or removable hard drives, to the network.

In an era where the digital landscape is continually evolving, ARU's commitment to strong cyber security policies is not only necessary but also a strategic imperative. By protecting sensitive data, mitigating cyber threats, and complying with relevant regulations, we reinforce our organisation's resilience and maintain the trust of our stakeholders. The benefits extend beyond risk reduction and cost savings to encompass improved operational efficiency and long-term sustainability. With these considerations in mind, ARU is dedicated to upholding and advancing its cyber security policies to secure our digital future.

Business Continuity & Disaster Recovery

Cybersecurity is an integral component of ARU’s Business Continuity Plan (BCP). ARU ensures that:

- backups are tested;
- recovery procedures are documented;
- failover systems are maintained;
- restoration times are monitored;
- critical systems have redundancy.

In the event of major cyber disruption, ARU activates the BCP.

RELATED DOCUMENTS

- *Confidentiality Policy.*
- *Acceptable use of Electronic Media Policy.*
- *Technology Procedures Manual.*

AUTHORISATION

Michael Wentworth

Managing Director
Apprenticeships Are Us Limited

DOCUMENT CONTROL

Version	Authorised by	Authorisation Date	Sections	Amendment
1.1	M. Wentworth	01/11/2022	All	N/A
1.2	M. Wentworth	07/11/2023	All	Cover page, information update
1.3	M. Wentworth	30/10/2024	All	Information update
1.4	M. Wentworth	19/12/2025	All	Information update