Toukley Neighbourhood Centre
Ph: 02 43961555 / Email: admin@tnc.org.au / Website: www.tnc.org.au
PO Box 55, Toukley NSW 2263 / ABN: 64 997 484 484 / Association No: Y02437-47

TNC is the heartbeat of a connected, supported, empowered, inclusive and thriving community. We partner with the broader community to share what we can and provide a hand up to those in need, so they can Wallamba-bayn (come back) and join us in delivering our vision.

POLICY - CYBERSECURITY

1. Policy Information

Title:	Cybersecurity
Effective Date:	19-Jan-2026
Policy Owner:	EO
Oversight:	R&CC
Next Review Date:	Jan-2027

1.1. Definitions

This policy uses the terms defined in the *TNC Master Definitions Table*, available on the Toukley Neighbourhood Centre website (www.tnc.org.au/policies).

Policy-specific definitions are listed below (if required).

Term	Explanation
Cybersecurity Incident	An event that compromises, is suspected of compromising, or attempts to compromise the confidentiality, integrity or availability of TNC systems, data or accounts.
RBAC	Role-Based Access Control, where access permissions are based on job role and restricted to the minimum required for duties.
Multi-Factor Authentication (MFA)	A security control requiring more than one method to verify identity when accessing systems.
Patch	A software update that fixes security vulnerabilities or other issues in applications or operating systems.
IT Support Provider	The external vendor or provider engaged by TNC to deliver technical support, monitoring and cybersecurity services.

1.2. Context

At Toukley Neighbourhood Centre (TNC), policies are developed in alignment with the *TNC Policy Framework* and support the delivery of safe, effective and accountable community services.

TNC policies are developed to:

- Assist TNC to meet its organisational objects and manage risk effectively
- Support staff and volunteers in performing their duties
- Demonstrate how TNC meets its governance, compliance and quality expectations
- Provide clarity, transparency and consistency across all areas of TNC operations.

This policy forms part of TNC's risk and governance system and supports the ongoing protection of TNC's systems, devices, accounts and data from cyber threats.

This policy must be read in conjunction with the Risk Management Policy, the Incident Management Policy, and the Records Management Procedure.

TNC is bound by the *Australian Charities and Not-for-profits Commission Act 2012 (Cth)* and regulated by the *ACNC*.

1.3. Related Documents

- Risk Management Policy
- Incident Management Policy
- Privacy and Data Protection Policy
- Records Management Procedure
- Asset Register
- Cybersecurity Incident Response Plan

1.4. Change Control

Effective Date	Author	Approver	Comments
12-Dec-2023	Bronwyn Evans	BoM	Initial document
08-Apr-2024	Bronwyn Evans	BoM	Updates arising from Loyal IT review of policy
09-Dec-2024	Donna Tudman	BoM	Annual review and minor refinements to RACI
08-Dec-2025	Bronwyn Evans	BoM	• Applied new template • CM ➔ EO • Removed measurement criteria
19-Jan-2026	Bronwyn Evans	BoM	• Introduced explicit BYOD controls to reduce cyber risk associated with personal devices accessing TNC systems and data.

1.5. Contents

2. Policy Overview

2.1. Purpose

This policy establishes TNC's approach to protecting its systems, devices, accounts and data from cybersecurity threats. It sets out the minimum requirements for safeguarding information, ensuring continuity of operations, and maintaining the security and integrity of digital environments used by TNC.

2.2. Overview

TNC relies on digital systems to deliver programs, manage information, communicate with stakeholders and meet governance and compliance obligations. Cybersecurity threats can compromise the confidentiality, integrity and availability of these systems and may result in significant harm to individuals, the organisation and the community.

TNC adopts a layered approach to cybersecurity, including preventative, detective and responsive controls. Core requirements include MFA, secure passwords, RBAC, secure devices, patching, backups, monitoring and timely reporting of cybersecurity incidents.

The EO and IT support provider maintain TNC's cybersecurity environment, monitor risks, and ensure systems and devices are protected to an appropriate standard. Staff and volunteers must use systems responsibly, protect credentials and devices, and report concerns promptly.

This policy must be read in conjunction with the Risk Management Policy and the Incident Management Policy.

There is no circumstance under which TNC systems, accounts or data may be accessed, stored or transmitted insecurely.

2.3. Scope

It applies to all:

- TNC-owned or managed devices (computers, tablets, phones, printers, network equipment)
- cloud services and online applications used by TNC
- email and communication systems
- digital accounts assigned to staff or volunteers
- data stored, transmitted or processed using TNC systems
- personal devices used to access TNC systems, where approved.

Policy-specific scope considerations include:

- MFA, passwords, account management and device configuration
- access control (RBAC), permissions and offboarding
- patch management, backups and monitoring
- cybersecurity incident detection, reporting and response.

3. Policy Principles

Policies always contain a set of principles that provide information relating to the rationale for the document. Staff and volunteers must consider and comply with these guiding principles when performing their duties.

Principle 1: Cybersecurity is a shared responsibility.

All individuals using TNC systems or data must contribute to maintaining a secure digital environment.

Principle 2: Access is controlled based on role and minimum necessary permissions.

RBAC ensures accounts and systems are only accessible by those with a legitimate operational need.

Principle 3: Strong authentication protects all systems and data.

MFA and secure passwords must be used across all accounts and applications.

Principle 4: Devices and systems must be kept secure at all times.

Approved device configurations, encryption, patching and antivirus controls must be maintained.

Principle 5: Cybersecurity incidents must be reported promptly.

Early reporting enables rapid containment and reduces harm.

Principle 6: Data must be stored, transmitted and disposed of securely.

Personal and sensitive information must be handled in accordance with privacy and records management requirements.

Principle 7: Offboarding processes must ensure timely removal of access.

Accounts and system permissions must be revoked immediately upon exit to prevent unauthorised access.

Principle 8: Monitoring and continuous improvement are essential.

Cyber risks, incidents and controls must be reviewed regularly and inform improvements to TNC's cybersecurity posture.

4. Roles and Responsibilities

4.1. Overview

Clear roles and responsibilities ensure that TNC policies are implemented effectively, monitored appropriately and aligned with governance expectations.

Accountability for policy application is shared across the organisation, with oversight provided by the designated committee identified in the Policy Information section.

The roles below outline who is responsible for complying with, implementing, and monitoring this policy. Specific responsibilities are clarified further through the RACI table.

Effective cybersecurity requires consistent application of security controls, responsible use of systems and timely reporting of concerns. The EO ensures systems, devices and applications used by TNC meet appropriate security standards and that cybersecurity risks and incidents are monitored and addressed. The EO also ensures that accounts, permissions and access are managed appropriately throughout onboarding, role changes and offboarding.

The IT support provider maintains system configurations, updates, monitoring tools, backups and endpoint protection measures, and assists in responding to cybersecurity incidents.

Program and Volunteer Coordinators ensure staff and volunteers understand cybersecurity expectations and use systems in accordance with this policy.

Staff and volunteers must protect their login credentials, follow cybersecurity requirements, use systems responsibly and report issues promptly.

The Oversighting Committee reviews cyber risks, incidents and control performance in line with the Risk Management Framework.

4.2. RACI

This RACI identifies who is **Responsible (R)**, **Accountable (A)**, **Consulted (C)** and **Informed (I)** for the activities required under this policy.

Activity	BoM	Oversighting Committee	EO	Program / Volunteer Coordinators	Staff and Volunteers
Generic Policy Activities					
Understand and comply with the policy	I	I	C	R	R
Implement policy requirements in daily operations	I	I	A	R	R
Maintain procedures and records required by the policy	I	I	A	R	R
Monitor compliance and identify issues	I	A	R	R	R
Report incidents, risks or non-compliance	I	C	A	R	R
Review policy effectiveness and recommend improvements	I	A	A	C	I
Approve policy revisions	A	C	R	I	I
Policy Specific Activities					
Maintain cybersecurity controls and standards	I	C	A	C	R
Manage user accounts, onboarding and offboarding	I	C	A	R	I

Activity	BoM	Oversighting Committee	EO	Program / Volunteer Coordinators	Staff and Volunteers
Ensure MFA, RBAC and password requirements are enforced	I	C	A	C	R
Implement device security, patching and monitoring	I	C	A	C	R
Store, transmit and dispose of data securely	I	C	R	R	R
Detect, report and respond to cybersecurity incidents	I	A	R	R	R
Review cyber risks and incidents monthly	I	A	R	C	I

5. Policy Guidelines

The policy guidelines outline the rules, expectations and minimum requirements that must be followed under this policy. These guidelines apply to all individuals covered in the Scope section and support consistent, safe and compliant delivery of TNC operations. Policy-specific guidelines are listed below.

- All accounts used to access TNC systems or data must be secured with MFA and strong passwords.
- Access must be granted based on RBAC and restricted to the minimum necessary for duties.
- Devices used to access TNC systems must be secured through approved configurations, encryption, patching and antivirus protection.
- Personal devices may only be used to access TNC systems where explicitly approved and must meet security requirements.
- Systems and applications must be kept up to date, with security patches installed promptly.
- Credentials (passwords, PINs, MFA methods) must be kept confidential and must not be shared.
- Data must be stored, transmitted and disposed of securely in accordance with privacy and records management requirements.
- Suspicious emails, messages, links or attachments must not be opened and must be reported immediately.
- Cybersecurity incidents, including suspected attempts, must be reported as soon as possible.
- Information must only be stored in approved locations and must not be downloaded or transferred to insecure storage or personal accounts.
- Remote access must be used responsibly and only through approved, secure methods.
- All staff, volunteers and contractors must comply with onboarding and offboarding processes to ensure appropriate access control.

5.1. Personal Devices (Bring Your Own Device – BYOD)

Personal devices (including laptops, tablets and mobile phones) may only be used to access TNC systems, accounts or data where explicitly approved by the EO.

Where approval is granted, the following minimum requirements apply:

- Access to TNC systems must occur only via a TNC-issued account protected by multi-factor authentication
- The device must be secured with a strong password, PIN or biometric lock and be configured to automatically lock when not in use
- The device operating system and applications must be supported, kept up to date and patched promptly
- Endpoint protection (anti-virus / anti-malware) must be installed and active
- TNC data must not be stored permanently on personal devices and must only be accessed or stored in approved TNC systems
- Personal email accounts, personal cloud storage and unauthorised applications must not be used for TNC business
- Lost, stolen or compromised devices used to access TNC systems must be reported immediately
- TNC may revoke access to systems or require additional controls where a personal device is assessed as posing unacceptable risk

Approval to use personal devices may be withdrawn at any time.

6. Processes

The processes describe how the requirements of this policy are applied in practice. They outline the key steps, actions and records needed to implement the policy effectively. Detailed procedures or work instructions, where required, are maintained separately and referenced from this section.

6.1. Cybersecurity Processes

Account Management

- Create, modify and remove user accounts in accordance with RBAC.
- Assign permissions based on minimum required access for duties.
- Remove all access immediately when a person exits TNC.
- Review access permissions regularly and update as roles change.

Authentication and Passwords

- Enforce MFA for all systems supporting TNC operations.
- Use strong passwords in accordance with system requirements.
- Change passwords promptly if compromise is suspected.

Device Security

- Configure devices to meet approved security settings, including encryption, screen locking, patching and antivirus protection.
- Install system and application updates promptly.
- Report missing, stolen or damaged devices immediately.

Data Security

- Store TNC data only in approved locations.
- Encrypt sensitive information where appropriate.
- Dispose of information securely in line with records management requirements.
- Do not download, email or transfer information to unauthorised locations or personal accounts.

Email and Communication Security

- Do not open suspicious links or attachments.
- Report phishing attempts and suspicious communications immediately.
- Avoid storing sensitive information in email where not required.

Monitoring and Detection

- Maintain monitoring tools to detect suspicious activity, malware, unauthorised access or policy breaches.
- Review logs, alerts and notifications as required.

Cybersecurity Incident Response

- Report all actual or suspected cybersecurity incidents as soon as possible.
- Record incidents in the Incident Register.
- Follow the Cybersecurity Incident Response Plan.
- Escalate material incidents through the Risk Management Framework.

Remote Access

- Use only approved secure methods to access TNC systems remotely.
- Protect devices used for remote access with passwords and encryption.
- Ensure remote sessions are logged out fully when no longer required.

Third-Party and Vendor Access

- Ensure third parties accessing TNC systems follow appropriate security requirements.
- Grant vendor access only when necessary and revoke access immediately when no longer required.

6.2. Recordkeeping Requirements

Records created under this policy must be stored in accordance with TNC's records management requirements. This includes ensuring records are complete, accurate, accessible to authorised personnel, and retained for the required period.

Records may include:

- account creation, modification and removal records
- access permissions and RBAC updates
- device configuration, patching and maintenance records
- cybersecurity incident reports and response documentation
- logs or reports generated by monitoring tools
- evidence of training or onboarding related to cybersecurity
- correspondence with third-party providers regarding security matters.