TNC Policy

Policy Details

Title:	Cyber Security
Effective Date:	09-Dec-2024
Policy Owner:	Centre Manager
Applies To:	All staff and volunteers
Next Review Date:	31-Dec-2025

Purpose

This policy sets out TNC's policy for protecting its electronic information from unauthorised access. TNC handles personal and sensitive information and must ensure due care is taken to protect this information.

Context

This policy has been developed in alignment with the TNC Policy Framework.

TNC Policy Documents are developed to:

- Assist TNC to meet the objects of the organisation and manage risk effectively
- Assist TNC staff and volunteers in performing their duties
- Outline how TCNC will meet governance expectations
- Provide transparency and clarity to TNC staff and volunteers.

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

Definitions

Term	Explanation
ACNC	Australian Charities and Not-for-profits Commission
BoM	Board of Management
CM	Centre Manager
RBAC	Role-Based Access Control
TNC	Toukley Neighbourhood Centre

Contents

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: TNC complies with the Privacy Act

Personal information and sensitive information are defined in the ***Privacy Act 1988*** (Cth) (the Privacy Act).

- *Personal information* is information or an opinion about an identified person (or a person that can reasonably be identified), regardless of whether the information or opinion is true or recorded in a material form.
- *Sensitive information* is a subset of personal information, and may include, for example, a person's religious or philosophical beliefs, sexual orientation or health information.

For more on what constitutes personal information and sensitive information, see the key concepts in the Australian Privacy Principles guidelines.

The Privacy Act has requirements for the way personal information and sensitive information are collected and stored. The Office of the Australian Information Commissioner's (OAIC) Australian Privacy Principles guidelines has information about these requirements.

ACNC has a guide on managing people's information and data, which provides information for charities about collecting, storing and using the information and data they hold about people in a responsible way.

Measurement Criteria

The measurement criteria to validate that this principle has achieved the desired outcomes are:

- Personal and/or sensitive information stored by TNC is not subject to data breach.

Principle 2: The technology and information assets that need to be protected are detailed in the Asset Register

The Asset Register records asset description, date purchased, purchase price, current depreciated value, program within which the asset is used and identifies the physical location of the asset and/or the person who is responsible for the asset.

Measurement Criteria

The measurement criteria to validate that this principle has achieved the desired outcomes are:

- All TNC technology and information assets are listed accurately and completely in the Asset Register.
- Appropriate controls are recorded in the Risk Register to ensure accuracy and currency of the Asset Register.

Principle 3: The threats to TNC's technology and information assets are recorded in the Risk Register

The Risk Register records each identified risk to TNC and has associated controls and/or treatment plans defined to manage, mitigate or monitor the risk, as appropriate. The risk of a cyber-attack is specifically listed in the Risk Register.

Refer to the Risk Management Policy for more information about risk assessment and the risk management framework used by TNC.

Measurement Criteria

The measurement criteria to validate that this principle has achieved the desired outcomes are:

- Risks relating to cyber security, along with appropriate controls and treatment plans are identified in the Risk Register.

Principle 4: This policy details the rules for protecting TNC's technology and information assets

Refer to Rules for Protecting TNC's Technology and Information Assets~~Rules for Protecting TNC's Technology and Information Assets~~ for these rules.

In addition, refer to the Risk Register and particularly the Controls Plans and Treatment Plans in Smartsheet.

Measurement Criteria

The measurement criteria to validate that this principle has achieved the desired outcomes are:

- Rules relating to cyber security are reviewed and appropriate controls and treatment plans are identified in the Risk Register.

Principle 5: TNC maintains a cyber security incident response plan that is reviewed regularly

An incident response plan helps you prepare for and respond to a cyber incident. It outlines the steps you and your staff need to follow.

Measurement Criteria

The measurement criteria to validate that this principle has achieved the desired outcomes are:

- The cyber security incident response plan is a mitigation identified with appropriate controls and treatment plans identified in the Risk Register.

Principle 6: TNC maintains a matrix of roles and responsibilities relating to cyber security management

Refer to the RACI matrix below.

Requirements	Board	CM	Program Staff	Volunteers	IT Vendor(s)
Approve Cyber Security Policy	Accountable	Responsible	Informed	Informed	Consulted
Facilitate education re cyber security best practices	Informed	Accountable	Informed	Informed	Consulted
Understand Cyber Security Policy	Responsible	Accountable	Responsible	Responsible	Consulted
Apply rules detailed in Cyber Security Policy	Responsible	Accountable	Responsible	Responsible	Responsible
Audit adherence to Cyber Security Policy	Accountable	Responsible	Informed	Informed	Consulted
Report cyber security incidents	Responsible	Accountable	Responsible	Responsible	Consulted
Manage cyber security incidents	Informed	Accountable	Responsible	Responsible	Consulted
Manage IT support to prevent cyber security incidents	Informed	Accountable	Informed	Informed	Consulted
Manage risks related to cyber security	Accountable	Responsible	Informed	Informed	Consulted
Manage RBAC	Informed	Accountable	Informed	Informed	Consulted
Manage Operating System and Applications patching	Informed	Accountable	Informed		Responsible
Manage application control	Informed	Accountable	Informed		Responsible
Manage data and applications backups	Informed	Accountable	Informed		Responsible

Rules for Protecting TNC's Technology and Information Assets

Passphrase Requirements

Staff and volunteers with access to TNC technology and information assets must use strong passphrases. Refer to the Australian Cyber Security Centre for information on how to create strong passphrases here: https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases/creating-strong-passphrases.

The principles explained on this page are:

- Use multi-factor authentication wherever possible.
- Use passphrases rather than passwords – passphrases are easier for people to remember and harder for machines to crack:
  - Create long passphrases. It is suggested that the passphrase is made up of at least four random words of at least 14 characters in total. Examples: "red house sky train", "sleep free hard idea", "crystal onion clay pretzel"
  - Create unpredictable passphrases. It is suggested NOT to use a lyric, quote or sentence as this could be predictable, because the language will follow grammar and punctuation rules (e.g. spaces between words, capital letter at the beginning, single character of punctuation at the end). Tip: open random pages in a book and select unrelated words.
  - Create unique passphrases for each valuable account. One way to reduce the burden of having unique passphrases for every valuable account is to use modifiers for each on based on the service that it relates to. Example: "crystal onion clay pretzel facebook".
- Secure your passphrases:
  - Use a password manager to store your passphrases. This will free you of the burden over remembering which passphrase applies to which system. Ensure that the password manager is from a reputable vendor, is maintained by the vendor with regular security updates and protect it with its own strong and memorable passphrase.
  - NEVER share a passphrase with anyone else.
- Protect what protects you:
  - Do not share your passphrases with anyone.
  - Be careful of your surroundings when using passphrases in public.
  - Only use trusted Wi-Fi, trusted telecommunications networks or a Virtual Private Network (VPN) when accessing valuable accounts. Note that free public Wi-Fi, without the use of a VPN, can potentially expose your browsing activity.
  - Log off and sign out of accounts when you finish using them.
  - Think critically when answering phone calls, messages and emails – are the senders really who they say they are. This link provides some useful tips: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/email-hardening/detecting-socially-engineered-messages
  - If a passphrase has been compromised, change it immediately and never use it again. You can check whether your email address has been compromised in a data breach here: https://haveibeenpwned.com/
  - If access to TNC data has been compromised, the CM must be notified immediately.

Email Security Measures

The following rules apply to use of email:

- All TNC staff and volunteers whose employment with TNC is longer than one month and Board are to have a specific email address assigned them. Permanent staff will be assigned Business Standard (paid) licensing and casual staff and Board will be assigned Business Basic (free) licensing.
- TNC email addresses are provided for the purpose of TNC business / activities. These should not be used for personal / private matters.
- Users should think critically when answering phone calls, messages and emails to confirm whether the senders are really who they say they are. This link provides some useful tips: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/email-hardening/detecting-socially-engineered-messages
- Only open email attachments from trusted contacts and businesses.
- All staff and volunteers using TNC technology and information assets are required to refresh their cyber security awareness via https://www.cyber.gov.au/learn-basics on an annual basis.

Sensitive Data Handling

The following rules apply to handling sensitive data:

- All staff and volunteers should be reminded of the definition of personal and sensitive data, per this policy.
- Access to sensitive staff and client data is on a "needs to know" basis.
- Physical files with sensitive data must be stored in a locked piece of furniture (e.g. drawers, filing cabinet) in a locked room.
- Electronic files containing sensitive data must be stored on SharePoint in secured folders that have appropriate limited access. These files should NEVER be stored on computer hard drives.
- Physical and electronic files containing sensitive data must be destroyed when these are no longer relevant.

Handling Technology

The following rules apply to handling of technology:

- Staff and volunteers must not access TNC confidential data in public places (e.g. a coffee shop) or places where non-TNC personnel can see the screen or hear interactions.
- TNC technology devices must be turned off and stored securely overnight (e.g. in a locked cabinet).
- Theft of loss of a TNC technology device must be notified to the CM immediately.
- Data must not be stored on technology device hard drives or removable devices. Always use cloud storage.
- Technology devices must be disposed of securely, ensuring the destruction of any hard data storage components.

Media Standards

The following rules apply to media enquiries, social media and internet access:

- Only authorised staff and volunteers are permitted to make public posts / comments using TNC social media accounts, and even then, a second authorised staff or volunteer must proof such posts.
- TNC emails should not be used publicly for personal causes / concerns / posts / etc.
- TNC technology devices should be used primarily for TNC-specific purposes, however, occasional reasonable use for personal purposes is acceptable. Examples of reasonable use include internet banking, access to web-based email programs, internet search.

Software Accounts

The following rules apply to use of software accounts:

- All TNC activities are to be conducted using official TNC email accounts as the username.

  This means that individual Gmail, google, Hotmail, etc accounts are not to be used. The CM is responsible for the secure storage of generic accounts, including passphrases which should use the rules above.

Role Based Access Control (RBAC)

Role based access control is essentially defining the minimum permissions to access information to allow each worker to do their job but nothing more.

A physical example of this is storing sensitive files in a filing cabinet where only authorised people have access to the key and then use of the files is supervised to ensure it is returned. In IT, permissions are given instead of keys to access data, systems, and accounts. This involves having a staff onboarding and offboarding process to manage these permissions as well as defining what each role in the organisation needs access to and what should be restricted from that role.

The CM is responsible for:

- Staff and volunteer onboarding and offboarding procedures
- Definition of permission requirements by role.

Operating System and Applications Patching

As software ages, users can find ways to use the software in unintended ways to gain unauthorised access to the application, operating system, or device.

Software that has the potential to be exploited is said to have vulnerabilities. Vulnerabilities for various software are announced and released in bulletins known as Common Vulnerabilities and Exposures (CVE) bulletins and publicly searchable on sites such as https://cve.mitre.org/. Each bulletin has a rating between 1-10 with 10 being mission critical and immediate action required.

Security patches are regularly released to patch out these vulnerabilities and unless actively managed by IT staff, organisation staff or patch management software, it can present a risk to your organisation.

Application Control

Application control refers to the application of security controls to restrict unauthorised changes in Windows and MacOSX, as well as restricting applications so they are only able to perform actions within their desired function and nothing unintended.

This can be done through security software such as antivirus and anti-malware, Settings and software policies and Operating System features such as Windows Defender and User Account Control.

Other examples may include one of the in-built solutions from Microsoft (e.g. AppLocker or Windows Defender Application Control) or it may be a third-party solution (e.g. AirLock Digital's AirLock, Ivanti's Device and Application Control, Trend Micro Endpoint Application Control or VMWare Carbon Black App Control). Restricting Microsoft office Macros also falls under this category of Cybersecurity Policy

Cyber Security Incident Response Plan

Prepare and Prevent

This policy contains details of TNC's proactive approach to cyber security management. The key aspects are:

- Educate staff and volunteers about cyber security
- Develop policies relating to cyber security
- Identify important financial, data and technology assets
- Assess cyber security risks and determine controls and treatments
- Define roles and responsibilities re cyber security
- Prepare this cyber security incident response plan.

Check and Detect

The controls identified and documented in the Risk Register are intended to check and detect instances where cyber security management requires additional treatment.

Unusual activity that may indicate a cyber security incident includes:

- accounts and your network not accessible
- passwords no longer working
- data is missing or altered
- your hard drive runs out of space
- your computer keeps crashing
- your customers receive spam from your business account
- you receive numerous pop-up ads.

If staff or volunteers think there may be a security incident, document evidence and report to the CM. The CM will make contact with IT Support and potentially report via https://www.cyber.gov.au/report-and-recover/report.

Identify and Assess

This involves:

- Find the initial cause of the incident and assess the impact it can be contained quickly
- Determine the impact of the incident on TNC
- Determine its effects on TNC and its assets if not immediately contained.

Respond

This involves:

- Limiting further damage of the cyber incident by isolating the affected systems. If necessary, disconnect from the network and turn off affected computers to stop the threat from spreading.
- Remove the threat.
- Recover from the incident by repairing and restoring systems to business as usual.

Review

This involves:

- Identify if any systems and processes need improving and make those changes.
- Evaluate the incident before and after, and any lessons learnt.
- Update the cyber security incident response plan based on the lessons learnt so that the response can be improved in case of future incidents.

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

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