Policy Name:

Cybersecurity Policy

Table of Contents

Policy Name: 1

1. Definitions 1

2. Purpose 2

3. Scope 2

4.Principles 2

5.Responsibilities 3

6. General Cyber Security Information 3

7. Cyber Security Risk Mitigation 3

8. Reporting 5

9. Compliance and Legal Obligations 5

Change History: 6

Acceptance Certificate: 6

1. Definitions

The following definitions apply to this policy and help ensure consistent understanding across the organisation.

1.1. **Board Member**: A Board Member is a person who has been appointed or elected to sit on The Canopy's Board of Management.
1.2. **Child**: A Child is any person under the age of 18 years.
1.3. **Child Safe Environment**: A Child Safe Environment is one where children are safe from harm, feel respected and included, and where the NSW Child Safe Standards are actively applied.
1.4. **Manager**: A Manager is any staff member with formal responsibility for supervising others, managing a program, team, or site, or making decisions about risks or incidents covered by this policy. This includes Executive staff where relevant.
1.5. **Staff**: Staff includes all employees of The Canopy, whether full time, part time, fixed term, or casual.
1.6. **Volunteer**: A Volunteer is a person who performs work or duties for The Canopy without pay, under an agreed role or arrangement.

2. Purpose

2.1. The Canopy's Cybersecurity policy establishes the framework for managing and protecting The Canopy's information assets, systems, and stakeholders from cyber threats, data breaches, and unauthorised access.

2.2. This policy ensures compliance with relevant Australian laws and demonstrates our commitment to safeguarding personal and organisational data. Its purpose is to preserve the confidentiality, integrity, and availability of information by preventing unauthorised access, use, disclosure, disruption, modification, or destruction.

2.3. This policy applies to all staff members, including employees, board members, independent contractors, and volunteers who access or manage The Canopy's digital systems and data.

2.4. This Cybersecurity policy is to be implemented in conjunction with the Canopy's IT Acceptable Use Policy, Data Breach Response Policy, Password Policy, and Risk Management framework.

2.5. By adhering to this Cybersecurity Policy, we ensure that our organisation maintains trust, protects our data, and complies with legal and regulatory obligations.

3. Scope

3.1. The Canopy's Cybersecurity Policy applies to all members of The Board, Chief Executive Officer, The Leadership Team, workers, students, volunteers, and sub-contractors who access or manage the Canopy's digital systems and data.

3.2. All employees, contractors, consultants, temporary workers, and third-party service providers.

3.3. All information assets owned, managed, or processed by the organisation, including digital and physical formats.

3.4. All systems, networks, devices, and services used to store, transmit, or access company data.

4.Principles

4.1 The Canopy believes Cybersecurity is everyone's responsibility.

4.2. The Canopy believes Cybersecurity is essential in safeguarding individuals and stakeholders against the growing risks and threat of cyber-attacks.

4.3. All personnel involved at The Canopy are responsible for ensuring information is secured and always protected.

4.4. All personnel involved in service provision and program delivery at the Canopy adhere to all Information Security policies, procedure's, systems, and processes.

5.Responsibilities

5.1. Board and Executive Management oversee cyber security strategy, risk management, compliance and ensuring resources are available to implement security controls.

5.2. All Staff are responsible for following this policy, attending training, following safe practices and reporting any security issues or suspicious activity.

5.3. IT and Security Team is responsible for developing and implementing security controls, maintaining security measures and control systems, monitoring threats, and responding to incidents.

6. General Cyber Security Information

6.1. **Key Cyber Security Terms**

6.1.1. **Multi-factor authentication (MFA):** A security measure requiring two or more proofs of identity to grant a person access.

6.1.2. **Phishing:** A cyberattack using email or text messaging to contact a person posing as a legitimate institution to lure individuals into providing sensitive information, passwords, or access information.

6.1.3. **Malware:** Software purposely designed to disrupt, damage, or gain unauthorised access to technology systems.

6.1.4. **Smart engineering:** A cyberattack relying heavily on human interaction to coerce individuals into breaching policy and set procedures, to gain access to systems, networks or physical locations.

6.1.5. **Cyber Security Incident:** Refers to an incident involving unauthorised impairment or attack that targets computer information systems, infrastructure, computer networks, or personal computer devices.

7. Cyber Security Risk Mitigation

7.1. **Internal Risks are mitigated by;**

7.1.1. Conducting regular, role-specific cyber security training for all staff.
7.1.2. Promoting awareness of phishing, social engineering, and human error risks.
7.1.3. Ensure staff know how to report suspicious emails or incidents.
7.1.4. Ensure staff are aware of internal and external reporting procedures and processes.

7.2. **External Risks are mitigated by;**

7.2.1. Use up-to-date firewall and anti-malware software.
7.2.2. Require multi-factor authentication (MFA) for all critical systems.
7.2.3. Regularly update and enforce strong password policies.
7.2.4. Monitor for suspicious activity using intrusion detection systems.

7.3. **Access Control**

7.3.1. Access to systems and data must follow the principle of **least privilege**.
7.3.2. Strong, unique paraphrases must be used as passwords and changed regularly.
7.3.3. Multi-factor authentication (MFA) is required where supported.
7.3.4. User accounts must be disabled promptly upon employee termination or role change.

7.4. **Physical and Environmental Security**

7.4.1. Secure areas must be protected with access controls (e.g., swipe cards, PINs).
7.4.2. Equipment must be locked or stored securely when unattended
.

7.5. **Acceptable Use**

7.5.1. Users must comply with the IT Acceptable Use Policy and all Information Security policies and procedures.
7.5.2. Company assets are to be used primarily for business purposes.
7.5.3. Personal devices may only be used for work purposes if explicitly approved and secured.

7.6. **Data Protection and Privacy**

7.6.1. All personal and sensitive data must be handled in compliance with applicable privacy regulations (e.g., Australian Privacy Act, GDPR).
7.6.2. Data must be encrypted during transmission and storage where appropriate.
7.6.3. Retention and disposal of data must follow documented procedures.

7.7. **Cyber Security Awareness and Training**

7.7.1. All staff, including board members and volunteers, will complete tailored, role related, cyber security awareness training bi-annually or as directed.

7.7.2. All staff will attend updated refresher training to maintain knowledge on evolving cyber threats and comply with regulatory changes and service expectations.

7.8. **Business Continuity and Backup**

7.8.1. Critical IT and data base systems and data must be backed up regularly.

7.8.2. Backups must be encrypted, tested, and stored securely.

7.8.3. Business continuity and disaster recovery plans must be reviewed and tested annually

7.9. **Third-Party and Vendor Security**

7.9.1. Vendors and third parties with access to company systems or data must be assessed for privacy and cyber security risks.

7.9.2. Contracts must include data protection, retention, data destruction, data breach and confidentiality clauses.

7.9.3. Third-party access must be limited, monitored, and revoked when no longer needed.

7.9.4. The Canopy will consider conducting privacy impact assessments for new projects or new providers.

8. Reporting

8.1. Any suspicious internet items or actions must be reported to the CEO or the responsible manager, Information Technology (IT) personnel and/or delegated personnel responsible for cyber security threats and risks.

8.2. Cybersecurity incidents and risks must be logged through the incident reporting process to ensure appropriate follow-up actions and future monitoring can occur.

8.3. All personnel associated with The Canopy will follow internal and external reporting obligations set out in the Cybersecurity Procedures, Data Breach Response Policies and Procedures, IT Acceptable Use Policy, Information Use Procedures, Privacy Policy, and Incident and Risk Management procedures.

8.4. Report a cybercrime, incident or vulnerability to protect the organisation and service users from further harm at cyber.gov.au/report

8.5. Report related data breaches to relevant legislative entities, including; the OAIC, NDB, ACSC and affected individuals as required.

8.6. Document and review all incidents to improve future responses.

8.7. Continuous improvement learning opportunities from incidents will be documented and addressed.

9. Compliance and Legal Obligations

9.1. The Canopy will comply with the Notifiable Data Breach (NDB) Scheme and the Cyber Security Act 2024.
9.2. The Canopy will report ransomware payments as required by law (if applicable).
9.3. The Canopy will align privacy and cyber security practices with the OAIC's guidelines.
9.4. The Canopy will review this policy and associated procedures regularly.

Document ID:	POL-031
Version:	1.0
Finalised date:	April 2026
Review date:	April 2028
Author – branch/unit/area:	Project Officer
Audience:	• Board • All Employees • Volunteers and Contractors
Related Legislation, Standards and Frameworks:	• Privacy and Personal Information Protection Act 1988 (NSW) • Cyber Security Act 2024 • 2023-2030 Australian Cybersecurity Strategy • Office of the Australian Information Commissioner (OAIC) • Notifiable Data Breach Scheme (NBD) • Australian Signals Directorate

Status:	Mandatory
Related Governance:	• Privacy Policy • Data Breach Response Policy • Risk Management Framework • Information Security Policy • IT Acceptable Use Policy • Password Policy • IT Systems and processes • Incident Report Policies and Procedures • Social Media Guidelines
Replaces:	N/A – New Policy

Change History:

Date	Change Description	Reason for Change	Author	Issue No:
1.05.2026	New Policy	Governance uplift to align with legal and contractual regulations	S. Hicks	1.0

Acceptance Certificate:

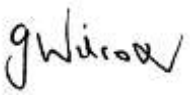
This policy is approved by:

☐ **Tier 1 – Board Approved Policy**
Requires formal approval by the Board.

☐ **Tier 2 – CEO Approved Policy**
Approved and authorised by the CEO.

☐ **Tier 3 – Executive Approved Procedure / Guideline**
Approved by relevant Executive Staff.

Approved Date: 24 June 2026

Signed: 

Name/Position: Gen Wilcox, CEO