Procedure Name:

Cyber Security Procedure

Document ID:	PRO-042
Version:	1.0
Finalised date:	May 2026
Review date:	May 2028
Author – branch/unit/area:	Project Officer
Audience:	• Board • All Employees • Volunteers and Contractors
Related Legislation, Standards and Frameworks:	• Australian Signals Directorate • Office of Australian Information Commissioner (OAIC) • Child Safe Scheme • The Commonwealth Privacy Act 1988 • Australian Privacy Principles
Status:	Mandatory
Related Governance:	• Cyber Security Policy • Data Breach Response Policy • Data Breach Response Procedure • IT Information Policy • Risk Management related governance • Privacy Policy • Complaints and Feedback Policy
Replaces:	N/A – New Procedure

Change History:

Date	Change Description	Reason for Change	Author	Issue No:
03.05.2026	New Policy. Full re-write.	New Procedure.	Suzanne Hicks	1.0

Acceptance Certificate:

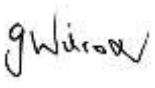
This policy is approved by:

☐ **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

Contents

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. **CEO:** Chief Executive Officer.
1.5. **Manager**: A Manager is any staff member with formal responsibility for supervising others, managing a program, team, or site, or making decisions about events covered by this policy. This includes Executive staff where relevant.
1.6. **Staff**: Staff includes all employees of The Canopy, whether full time, part time, fixed term, or casual.
1.7. **Volunteer**: A Volunteer is a person who performs work or duties for The Canopy without pay, under an agreed role or arrangement.
1.8. **Cyber Security Incident:** Refers to an incident involving unauthorised access, impairment or attack that targets computer information systems, infrastructure, computer networks, or personal computer devices.
1.9. **Personal information:** Personal Information is information about an identified individual, or an individual who is reasonably identifiable.

2. Purpose

2.1. The purpose of this Cyber Security Procedure is to provide information on the actionable steps of prevention, detection, response, and recovery processes expected to take place when a cyber security risk or incident has occurred.

2.2. This procedure provides guidance protect The Canopy's information assets, systems, clients, employees and stakeholder's information from cyber threats, cyber risks, data breaches, and unauthorised access.

2.3. This procedure accompanies the Cyber security policy ensuring the Canopy remains compliant with all relevant legislation, contractual agreements, and continues to safeguard information and organisational assets.

2.4. This procedure is based on best practices and recent legal reforms outlined in the cyber security policy. The structure ensures clarity, accountability, and compliance with the latest regulatory requirements.

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

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

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

2.8. By adhering to this Cybersecurity Procedure, 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 Procedure 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 takes its organisational responsibility to protect personal and organisational assets seriously and is committed to robust cyber security systems, policies and processes.

4.2. The Canopy believes Cybersecurity is everyone's responsibility.

4.3. The Canopy is aware that adequate management of cyber security threats and risks contributes to the overall trust and faith families, communities, governing entities and funding bodies have in our organisation's level of commitment to, and competence in, service excellence.

4.4. In the event of a cyber security threat, incident or risk, The Canopy will reduce the detrimental impact of the issue by effectively minimising the risk of harm to affected individuals, including

demonstrating accountability in the associated Incident Report and cyber security response plan.

4.5. The Canopy operates from principles of transparency, accountability, commitment to repair, and capacity building to mitigate future breaches. This is of particular importance when a cyber security threat or incident occurs that is likely to cause serious harm to affected individuals.

4.6. The Canopy values transparency and empowerment. The Canopy enables individuals to take steps to reduce their personal and professional risk of harm from cyber security threats and risks.

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

5. Responsibilities

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

5.2. All personnel associated with The Canopy are required to comply with all cyber security policies, reporting processes, role specific training and protect personal and organisational information assets. This is inclusive of understanding their individual role in cyber security.

5.2 **The Board**

The Board of The Canopy is ultimately responsible for all legal, regulatory, contractual obligations and corporate governance systems relating to information security and data management systems.
The Board hold responsibility for resourcing the operationalising of the Cyber Security Policy, Procedures and Response Plans. This includes associated Information Security policies and procedures.
Board and Executive Management oversee cyber security strategy, risk management, compliance and ensuring resources are available to implement security controls.

5.3 **Chief Executive Officer**

The Chief Executive Officer (CEO) is accountable to The Board in the development and maintenance of a strong and resilient cyber security culture across all service areas.
The Chief Executive officer provides leadership and oversight responsibility of all cyber security information technology systems are embedded into service delivery in alignment with legislative and operational requirements.
The Chief Executive Officer holds responsibility for overseeing a dedicated response team/ or personnel to manage containment, risk mitigation, and communication efforts, with a focus on preventing future cyber security incidents and maintaining detailed incident and risk records.

5.4 **Leadership Team**

The Leadership team oversee the implementation of the Cyber Security Procedure, associated risk management frameworks, data breach measures, policies, procedures and Information Technology systems of The Canopy.

5.5 **All Staff and Volunteers**

All workers and volunteers are required to report any suspected cyber security threats or actual risks to the CEO, Leadership Team or a member of the Board immediately after finding of the issue.
All staff and volunteers are expected to comply with cybersecurity training, follow established security protocols to prevent data breaches, and adhere to all cyber security processes and procedures.

5.6. **IT and Security Team** are responsible for developing and implementing security controls, maintaining security measures and control systems, monitoring threats, and responding to

incidents.

6. Key Cyber Security Terms

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

6.2. **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.

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

6.4. **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.

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

6.6. **Proactive Protection:** Implement technical and organisational measures to prevent cyber incidents.

6.7. **Rapid Response:** Ensure quick and effective action in the event of a cyber incident or data breach.

6.8. **Compliance:** Adhere to the Cyber Security Act 2024, Notifiable Data Breach Scheme, Privacy Act 1988 (Cth), the, and other relevant regulations.

6.9. **Continuous Improvement:** Regularly review and update cyber security policies, procedures and operational practices.

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 complex unique passphrases – replacing old passwords.
7.2.4. Monitor for suspicious activity using intrusion detection systems.
7.2.5. Create secure backups and back up data regularly.

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. **Security Awareness and Training**
7.7.1. All staff, including board members and volunteers, will complete tailored, role related, security awareness training bi-annually or as directed.
7.7.2. All staff will attend updated refresher training to maintain knowledge on evolving threats and comply with regulatory changes and

7.8. **Business Continuity and Backup**
7.8.1. Critical 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.Procedure and Reporting

8.1. All suspected or actual security incidents must be reported immediately to the relevant Service Manager, CEO, Information Technology (IT) personnel and/or security management staff. This includes any suspicious internet activity, emails or related on-line action.

8.2. A Cybersecurity Incident Report and response plan must be developed and followed outlining roles, contact details, and steps for containment, assessment, notification, and review.

8.3. The CEO or Managerial delegate will report notifiable cyber security threats, risks and/or data breaches to the OAIC and affected individuals as required.

8.4. The CEO or Managerial delegate will notify relevant legislative bodies when required (e.g., ACSC, Australian Federal Police) in the event of significant incidents.
8.5. The CEO or delate will document and review all incidents to improve future responses.
8.6. Continuous improvement learning opportunities from cyber security incidents will be documented and addressed.
8.4. All personnel associated with The Canopy will follow internal and external reporting obligations set out in the Cybersecurity Policy, Data Breach Response Policies and Procedures, IT Acceptable Use Policy, Information Procedures, Privacy Policy, and Incident and Risk Management procedures.

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.