CYBER SECURITY GOVERNANCE POLICY

Policy Category: Governance & Risk Management	**Version: One (supersedes V2 - Apr 2025)**
Drafted By: P. Pynor, revised by M.Graetz	**Approved by Board on 31 March 2026**
Responsible Person: Cyber Security Officer	**Scheduled Review Date: 31 March 2028**

Part A - Cyber Security Governance Policy

Introduction

One Foundation International (OFI) is committed to maintaining high standards of integrity, accountability, and risk management in the stewardship of its information, systems, and digital assets. In line with the expectations of the Australian Charities and Not-for-profits Commission (ACNC), the Board recognises cyber security as a material governance and operational risk that requires ongoing oversight.

OFI utilises a combination of internal controls and external specialist services, including proactive cyber risk monitoring and incident response services made available through its cyber insurance arrangements. These services assist in identifying vulnerabilities, emerging threats, and potential incidents; however, they do not replace OFI's own responsibility to manage cyber risk.

Governance Statement: The Board retains ultimate accountability for cyber security risk management. Reliance on third-party services, including insurers, does not diminish OFI's responsibility to protect its systems, information, beneficiaries, donors, and stakeholders.

Purpose

The purpose of this policy is to establish a formal governance framework for information security and cyber safety. The policy sets out minimum standards, responsibilities, and procedures to protect OFI's information systems, including systems and content created by or with the assistance of artificial intelligence (AI), from unauthorised access, misuse, loss, corruption, or exploitation.

Objectives

This policy seeks to ensure that OFI:

- Protects the confidentiality, integrity, and availability of information assets
- Safeguards personal, financial, and sensitive data relating to donors, beneficiaries, partners, and personnel
- Reduces exposure to cyber threats, fraud, and operational disruption
- Promotes responsible and ethical use of digital technologies, including AI tools
- Maintains appropriate Board oversight of cyber security and technology-related risks

- Responds promptly and effectively to cyber incidents
- Complies with applicable legal, regulatory, contractual, and insurance obligations
- Preserves public trust and organisational reputation

Scope

This policy applies to all individuals who access, manage, or use OFI information systems or data, including:

- Board Directors
- Employees
- Contractors and consultants
- Volunteers
- Third-party service providers and vendors

The policy applies to all OFI information assets and systems, whether owned, leased, or hosted by third parties, including computers, mobile devices, cloud services, email systems, websites, financial systems, databases, and AI-enabled tools.

Policy Statement

All information created, stored, processed, or transmitted using OFI systems is the property of OFI unless otherwise required by law or contract. While OFI respects reasonable personal privacy, users should have no expectation of absolute privacy when using organisational systems.

OFI reserves the right, to the extent permitted by law, to monitor, audit, and review systems and network activity for security, compliance, and risk management purposes. Proactive monitoring and threat detection services provided through OFI's cyber insurer may be used to support these objectives.

Non-compliance with this policy may result in disciplinary action, termination of engagement, and/or referral to external authorities where appropriate.

Governance Roles and Responsibilities

Board of Directors

- Provide strategic oversight of cyber security and information risk
- Approve and periodically review this policy
- Ensure that cyber risks are considered within the organisation's broader risk management framework
- Ensure appropriate cyber insurance coverage is maintained

Cyber Security Officer (CSO)

- Implement and coordinate cyber security controls and procedures
- Maintain awareness of emerging cyber risks and threats
- Coordinate cyber incident response, including insurer and regulator engagement
- Promote cyber security awareness and compliance across the organisation

Personnel and Authorised Users

- Comply with this policy and related procedures
- Protect organisational information and systems from unauthorised access or misuse
- Use strong authentication practices and protect access credentials
- Remain alert to phishing, social engineering, and cyber fraud
- Immediately report suspected or actual cyber incidents

Where uncertainty exists, users must seek guidance from the CSO or Executive Officer.

Information Classification and System Taxonomy

OFI applies a risk-based approach to information and system classification rather than maintaining rigid or exhaustive system lists. Classification decisions are based on the sensitivity, criticality, and potential impact of unauthorised access, loss, or disruption.

For governance purposes, systems and information are broadly categorised as:

- **Red:** Highly confidential or mission-critical systems and data
- **Green:** Non-confidential systems that provide access to Red systems
- **White:** Isolated, non-sensitive internal systems
- **Black:** Externally accessible systems containing non-sensitive information

Security controls, access restrictions, and monitoring requirements are applied proportionately and may be adjusted as risks evolve.

Data Lifecycle Management, Protection, and Privacy

Information must be managed throughout its lifecycle in accordance with OFI's Data Retention & Destruction Policy and applicable privacy laws.

Users must:

- Access only information necessary to perform their duties
- Store sensitive information in approved systems and locations
- Ensure data is retained only for lawful and legitimate purposes
- Securely destroy or de-identify information when no longer required

While OFI implements reasonable administrative, technical, and physical safeguards, no system can be guaranteed to be completely secure.

Responsible Use of Artificial Intelligence

The use of AI tools must be lawful, ethical, and aligned with OFI's values and risk appetite. Personnel using AI tools must ensure that:

- AI outputs are reviewed and verified prior to use or publication
- Confidential, personal, or sensitive information is not entered into public or unmanaged AI systems
- Intellectual property and copyright obligations are respected
- AI-generated or AI-assisted content does not mislead, defame, or cause reputational harm

Third-Party and Supply Chain Security

Third-party service providers with access to OFI systems or information must implement appropriate security safeguards. Where reasonably practicable, OFI will seek assurance that providers comply with relevant privacy, security, and contractual obligations.

Financial Fraud Prevention

To mitigate cyber-enabled fraud, any request to change banking details, payment instructions, or authorisations must be independently verified using a trusted secondary communication channel.

Data Backup and Business Continuity

Cloud-Based Data Storage and Recovery
OFI operates a cloud-first data environment. Organisational information is created and stored within approved cloud-based platforms rather than on local endpoint devices. Desktop and laptop computers are used as access tools only and are not relied upon as primary data stores.

Accordingly, OFI's data protection, backup, and recovery arrangements focus on the resilience and security of cloud-hosted systems. These arrangements include:

- Maintaining secure and continuous access to approved cloud platforms
- Protecting user and administrator accounts through strong authentication controls
- Preventing, detecting, and responding to unauthorised access, deletion, or corruption of data
- Restoring data or system access following a cyber incident, service disruption, or user error

Local device backups are not required where organisational data is not stored locally. Backup and recovery practices must remain consistent with insurer expectations and the organisation's cyber risk profile.

Board Assurance Statement
The Board notes that OFI's reliance on cloud-based data storage is appropriate to the organisation's size, operations, and risk profile, and is supported by access controls, incident response arrangements, and cyber insurance coverage.

Cyber Incident Reporting

A cyber incident includes any suspected or confirmed unauthorised access, system compromise, malware infection, phishing attack, data breach, or attempted or actual cyber fraud.

All cyber incidents must be reported immediately to the CSO. Delayed reporting may compromise OFI's ability to respond effectively and may impact insurance coverage.

Cyber Insurance Governance

OFI maintains cyber insurance coverage appropriate to its size, activities, and risk profile.

Role of the Cyber Insurance Policy

- **Layer 1 – Proactive Prevention:** Identification of vulnerabilities and threat alerts during the policy period
- **Layer 2 – Incident Response Expertise:** 24/7 access to coordinated legal, forensic, technical, and crisis response services
- **Layer 3 – Management Liability Protection:** Cover for Board members and senior executives for insured claims arising from cyber events

Mandatory Insurance Conditions
To preserve coverage, OFI must comply with insurer requirements, including:

- **72-Hour Consent Rule:** Emergency response costs may be incurred without prior written consent only within the first 72 hours following discovery of a cyber event (excluding ransom or extortion-related costs)
- **Ransomware and Extortion:** No negotiation or payment without the insurer's express written approval
- **Law Enforcement Notification:** Cyber-crime incidents involving fraud, theft, or extortion must be reported to appropriate authorities
- **Supply Chain Evidence:** Written confirmation must be obtained from third-party providers regarding the cause and duration of outages or incidents relevant to a claim

Prompt notification enables access to specialist support and protects insurance entitlements.

Review

This policy will be reviewed by the Board at least annually, or earlier if required due to material changes in risk, technology, or regulatory expectations.

Related Documents

- Risk Management Policy
- Privacy Policy
- Electronic Banking Signatory Policy
- Financial Controls and Fraud Prevention Procedures
- Cyber Incident Response Procedures (Part B)
- Cyber Risk Register

AUTHORISATION

Approved by the Board of Directors of One Foundation International.



Michael Chant
Board Chair

Date: 31 March 2026

Part B - Cyber Incident Response Procedures

These procedures provide operational guidance to support timely and consistent responses to cyber incidents in accordance with Part A governance requirements and insurance obligations.

Core Controls

- Strong password practices and use of multi-factor authentication where available
- Ongoing cyber awareness and phishing vigilance
- Responsible and authorised use of organisational technology
- Secure handling and transmission of sensitive information
- Controlled and monitored third-party access

Cyber Incident Reporting

In the event of a suspected cyber security incident (including ransomware, unauthorised access, phishing compromise, or data breach), staff must immediately notify the Cyber Security Officer (CSO). The CSO will then notify the Executive Officer or Admin Manager and, if required, the organisation's cyber insurance broker/insurer in accordance with policy conditions.

Reporting contacts:

Insurance broker: Aon

Insurer: CFC Underwriting Limited

Incident reporting methods: CFC Response (mobile app) or

24/7 Cyber Incident Response Hotline: **1800 803 202**

Incident Response Process

Personnel must not attempt to investigate, remediate, or resolve a suspected cyber incident independently unless expressly directed by the CSO.

1. **Identify:** Recognise indicators of compromise or suspicious activity (e.g., unusual system behaviour, unexpected emails, unauthorised access).
2. **Report:** Notify the CSO or a Director immediately (preferably within 1 hour). Preserve all relevant evidence.
3. **Contain:** Follow instructions provided by the CSO to limit further impact. Do not attempt independent remediation.
4. **Notify Insurer:** Record incident details, affected systems, and actions taken using the organisation's incident log.
5. **Document:** Record incident details, systems affected, and actions taken.

A detailed Cyber Incident Response Checklist is maintained separately by the Cyber Security Officer and may be updated from time to time without Board approval.

Part C - Cyber Insurance Incident Response Protocol

This Protocol sets out mandatory insurer notification and compliance requirements. It applies in addition to the Cyber Incident Response Procedures and must be followed to preserve cyber insurance coverage.

- Report incidents via the CFC response app or 24/7 response line provided by CFC Underwriting Limited
- Comply with the 72-hour insurer consent rule
- Adhere to all ransom, law enforcement, and supply chain evidence conditions

Failure to comply may affect insurance coverage.

Cyber Risk Register

The Cyber Risk Register is maintained as a separate document by the CSO and reviewed regularly by the Board. Each identified risk is assigned an owner, likelihood, impact, and mitigation strategy. The register is updated following incidents or material changes to OFI's cyber risk profile.