CYBER SECURITY POLICY

Policy: Cyber Security Policy	**Version: Two**
Drafted By: P Pynor	**Approved by Board on April 15, 2025**
Responsible Person: Board Chair	**Scheduled Review Date: July 14, 2027**

Introduction

While One Foundation International wishes to foster a culture of openness, trust, and integrity, this can only be achieved if external threats to the integrity of the One Foundation International systems are controlled, and the organisation is protected against the damaging actions of others.

Purpose

2.1 This policy sets out guidelines for generating, implementing and maintaining practices that protect the One Foundation International cyber media – its computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

2.2 This policy applies to employees, contractors, consultants, and volunteers at One Foundation International, including all personnel affiliated with third parties, to all equipment owned or leased by One Foundation International, and to all equipment authorised by One Foundation International for the conduct of the One Foundation International business.

Policy

3.1 While One Foundation International wishes to provide a reasonable level of personal privacy, users should be aware that the data they create on the One Foundation International systems remains the property of One Foundation International. Because of the need to protect One Foundation's network, the confidentiality of information stored on any network device belonging to One Foundation International cannot be guaranteed, and One Foundation International reserves the right to audit networks and systems periodically to ensure compliance with this policy.

3.2 Information in the possession of the One Foundation shall be classified into different grades depending on its degree of confidentiality. Particularly sensitive information will receive special protection.

3.3 Employees and volunteers will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.

3.4 Breach of this policy by any employee may result in disciplinary action, up to and including dismissal.

Responsibilities

1.1 It is the responsibility of the board to ensure that:

- staff are aware of this policy;
- any breaches of this policy coming to the attention of management are dealt with appropriately;
- a cyber security officer is appointed.

1.2 It is the responsibility of the cyber security officer to ensure that:

- the board is kept aware of any changes to the One Foundation International cyber security requirements;
- a report on the One Foundation International cyber security is submitted annually to the board.

1.3 It is the responsibility of all employees and volunteers to ensure that:

- they familiarise themselves with cyber security policy and procedures;
- their usage of cyber media conforms to this policy.

1.4 In the event of any uncertainty or ambiguity as to the requirements of the cyber security policies or procedures in any particular instance, employees and volunteers should consult their supervisor.

Processes

Monitoring

2.1 The board may authorise individuals with responsibility for cyber security issues in the organisation, including the cyber security officer, to monitor the organisation's equipment, systems and network traffic at any time for security and network maintenance purposes.

Confidentiality

2.2 Following consultation with the cyber security officer, the board shall from time-to-time issue cyber security procedures appropriate to different levels of confidentiality.

2.3 The organisation shall classify the information it controls in the organisation's computer system files and databases as either non-confidential (open to public access) or confidential (in one or many categories).

2.4 The cyber security officer is required to review and approve the classification of the information and determine the appropriate level of security that will best protect it.

System Taxonomy

Security level	Description	Example
Red	This system contains confidential information – information that cannot be revealed to personnel outside the company. Even within the company, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life-threatening consequences and/or an adverse financial impact on the business of the company.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information
Green	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access server and application(s). Management workstations used by systems and network administrators.

White	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
Black	This system is externally accessible. It is isolated from RED and GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public web server with non-sensitive information.

Data taxonomy

Security level	Description	Example
Red	Client data allowing financial exploitation or identity theft Organisation data allowing banking or financial exploitation	Client credit card and banking data Organisational credit card and banking data Client details that would facilitate phishing

Data Lifecycle Integration

All digital systems and user activities must comply with One Foundation's **Data Retention & Destruction Policy**, which outlines the appropriate duration, storage, and destruction of data. Data should not be retained beyond its necessary business or legal life and must be destroyed securely, as per data classification levels.

AUTHORISATION

Michael Chant
Acting Board Chair

ADDENDUM – NOTIFIABLE DATA BREACHES

What is a Notifiable Data Breach?

Under the Privacy Act 1988, an organisation must report a data breach when:

- Personal information is accessed, disclosed, or lost without authorization
- It is likely to result in serious harm to individuals
- The organisation hasn't been able to prevent that risk

Step-by-Step: Reporting a Notifiable Data Breach

1. Identify the Breach

As soon as you suspect a data breach:

- Take immediate steps to contain it (e.g., secure systems, reset passwords)
- Document what's happened
- Notify your internal stakeholders (e.g., board, IT support)

2. Assess the Breach (within 30 days)

Determine:

- What kind of personal information was involved (e.g., names, addresses, donation details, payment info)
- Who is affected and how many people
- Whether the breach is likely to cause serious harm (e.g., identity theft, fraud, distress)

If there is no likely serious harm, no notification is needed — just record the incident.

3. Notify Affected Individuals

If serious harm is likely, notify the individuals:

- Explain what happened
- Describe the data involved
- Recommend steps they can take (e.g., change passwords, monitor accounts)
- Provide your contact details for support

4. Notify the OAIC

Use the official OAIC NDB Form online: 🔗 Notify the OAIC of a Data Breach

You'll need to provide:

- Your organisation's details (ABN, ACNC status, contact person)
- Description of the breach
- Types of information involved
- Estimated number of individuals affected
- Steps taken to contain the breach
- How you've notified the affected people

What to Keep on File

Even if a breach isn't notifiable, you should document:

- When it happened
- What information was involved
- Who assessed the risk
- Why it wasn't reported
- Steps taken to prevent future incidents

Final Tip: Have a Breach Response Plan

Even a simple one-pager that includes:

- Who to call (e.g., IT, legal, board chair)
- A checklist of what to assess
- Your internal contact person for the OAIC form

DATA BREACH RESPONSE FORM

This document outlines the steps to take in the event of a suspected or confirmed data breach, in accordance with the Notifiable Data Breaches (NDB) Scheme under the Privacy Act 1988.

Step 1: Contain the Breach

- ☐ Immediately isolate affected systems or services.
- ☐ Disable compromised user accounts or access permissions.
- ☐ Secure physical areas related to the breach.
- ☐ Notify the Data Breach Response Team or relevant board/IT support.

Step 2: Assess the Breach

- ☐ What type of information was involved?
- ☐ Who is affected (number and types of individuals)?
- ☐ Is the breach likely to result in serious harm?
- ☐ What steps have already been taken?
- ☐ Complete assessment within 30 calendar days.

Step 3: Notify Individuals and OAIC

- ☐ If serious harm is likely, prepare a notification to affected individuals:
  - What happened
  - Type of information involved
  - Recommended actions
  - Contact details for further assistance

- ☐ Notify the OAIC using the official form: https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach

Step 4: Review and Prevent Future Breaches

- ☐ Document lessons learned from the incident.
- ☐ Update security measures, procedures, or training programs.
- ☐ Review and revise this response plan if necessary.

Internal Contacts

Data Breach Coordinator: _____

IT Support / Consultant: _____

Board Chair / Governance Contact: _____