TASMAN
ENVIRONMENTAL TRUST

CYBERSECURITY POLICY

Policy number	11	Version	1
Drafted by	Marios Gavalas	Approved by Board on	October 2023
Responsible person	Sky Davies	Scheduled review date	April 2025

INTRODUCTION

This policy outlines the cybersecurity guidelines and best practices for TET, acting as a charitable organization operating within New Zealand. In an increasingly digital world, it is crucial for charities to prioritize cybersecurity to protect their sensitive information, maintain donor trust, and ensure the uninterrupted delivery of their services.

SCOPE

This policy aims to establish a framework for implementing robust cybersecurity measures and creating a secure IT environment for TET's activities.

TET will:

1. Risk Assessment

1.1 TET is aware there are risks and will therefore conduct (via a 3rd party) a comprehensive risk assessment to identify potential cybersecurity threats and vulnerabilities specific to the organization.
1.2 TET will be satisfied the 3rd party processes are robust.
1.3 Review and update the risk assessment to adapt to evolving cyber threats and changes to align with emerging threats, technological advancements, and legal or regulatory requirements.

2. Governance and Leadership

2.1. Designate a responsible individual or contractor accountable for overseeing cybersecurity measures.
2.2. Develop and document a cybersecurity governance framework to ensure clear roles, responsibilities, and reporting lines.
2.3. Ensure Board are informed of breaches and actions on cybersecurity matters.

3. Access Controls

3.1. Implement access controls to ensure that only authorised personnel have access to sensitive information.
3.2. Ensure strong passwords including regular password changes (where necessary eg financial) and the use of complex passwords.
3.3. Implement multi-factor authentication for accessing critical systems or sensitive data.

4. Employee Education and Awareness

4.1. Provide regular cybersecurity training and awareness programs to all staff members, where needed (see Appendix 3)
4.2. Educate employees about social engineering attacks, phishing, malware, and other common cyber threats.
4.3. Encourage employees to report any suspicious activities or potential security incidents promptly.

5. Data Protection and Privacy

5.1. Comply with relevant data protection and privacy laws (see Appendix 1)
5.2. Establish procedures for handling and safeguarding personal and sensitive information, including encryption where appropriate.

6. Incident Response and Business Continuity

6.1. An incident response plan is outlined in Appendix 2 below, describing the steps to be taken in the event of a cybersecurity incident.

7. Contractor Management:

7.1. Ensure due diligence when selecting and contracting with third-parties.
7.2. Include cybersecurity requirements and obligations in contracts and agreements.

8. Monitoring and Auditing

8.1. Conduct internal and external cybersecurity audits to assess compliance with policies and procedures. This can form part of the policy regular review cycle.
8.2. Continuously review and update cybersecurity practices based on emerging threats and industry best practices.

Appendices

Appendix 1 | Legislation

Privacy Act 2020
The Privacy Act sets out rules for how organizations handle personal information. It includes provisions related to data breaches, privacy principles, and the obligations of agencies regarding the collection, use, and disclosure of personal information.

Harmful Digital Communications Act 2015
This legislation addresses harmful digital communications, such as cyberbullying, harassment, and online stalking. It provides mechanisms for dealing with such harmful content and establishes the role of the Approved Agency in resolving complaints.

Crimes Act 1961
The Crimes Act covers various offenses related to cybercrime, including unauthorized access to computer systems, unauthorized modification or impairment of data, and offenses related to the use of technology in fraud, identity theft, and forgery.

Telecommunications (Interception Capability and Security) Act 2013
This act focuses on the interception of telecommunications and ensures that service providers have the capability to assist government agencies with lawful interception and have appropriate network security measures in place.

Cyber Security Strategy and Action Plan
While not a specific legislation, New Zealand has a national cybersecurity strategy and action plan that outlines the government's approach to cybersecurity and sets objectives for improving cybersecurity resilience across the country.

Health Information Privacy Code
The Health Information Privacy Code, issued under the Privacy Act, provides specific privacy requirements for the health sector, ensuring the protection of personal health information and the rights of individuals.

Financial Markets Conduct Act 2013
This legislation covers the regulation of financial markets in New Zealand and includes provisions related to cybersecurity and data protection for financial service providers.

TET recognizes it is essential for organisations, including charitable ones, to be aware of these laws and regulations and ensure compliance with the relevant requirements to protect personal information, prevent cybercrime, and maintain the security and privacy of individuals' data.

TASMAN
ENVIRONMENTAL TRUST

Appendix 2 | Incident Response Procedure

1. Introduction

This Incident Response Plan outlines the procedures and guidelines to be followed in the event of a cybersecurity incident occurring within TET.

The primary goal of this plan is to effectively and efficiently respond to any cybersecurity incident, minimise its impact, and ensure the continuity of critical business operations. The plan defines roles and responsibilities, incident identification and classification, containment, eradication, recovery, and lessons learned.

2. Incident Response Team (IRT)

The Incident Response Team (IRT) consists of designated individuals responsible for managing and coordinating the response to cybersecurity incidents. For TET this be a third party contractor.

3. Incident Identification and Classification

Identification: Incidents can be detected through various means such as security monitoring, user reports, anomaly detection, or third-party notifications. Any employee who suspects a cybersecurity incident must report it immediately to the Trust Manager or Operations Manager (TET Manager).

Classification: The TET Manager will promptly classify the incident based on its severity and potential impact using the following categories:

Low:	Limited impact on operations and data confidentiality.
Medium:	Partial disruption to operations or compromise of sensitive data.
High:	Significant disruption or data compromise requiring immediate action.

4. Incident Response Process

A. Initial Response
Upon incident detection, the TET Manager shall notify the third-party contractor immediately to initiate a follow up. Their response may includean initial assessment taking necessary short-term actions, such as isolating affected systems from the network or disabling compromised accounts.

B. Investigation and Analysis
The 3rd party contractor shall conduct a thorough investigation to understand the nature and scope of the incident. They will preserve relevant evidence and logs for further analysis and potential legal actions.

They will determine the root cause and the extent of the impact on systems, data, and users.

C. Eradication and Recovery
The 3rd party contractor will develop a detailed plan to eradicate the threat and restore affected systems. They will implement the plan and verify the success of eradication.
Data backups, if available, will be used for system restoration.
Systems will be tested before reconnecting them to the network.

D. Communication and Notification
The TET Manager will manage all external communications to ensure accurate, timely, and consistent messaging.
If the incident involves personal data, the TET Manager, in association with any third party advisors, will assess the need for notifying affected individuals and regulatory authorities, as required by New Zealand's privacy laws.

E. Documentation and Reporting
Throughout the incident response process, all actions and findings will be thoroughly documented.

A post-incident report will be prepared, including a detailed analysis of the incident, response actions taken, and recommendations for improving the incident response process, within 1 month.

5. Lessons Learned

After the incident has been resolved, the 3rd party contractor will conduct a thorough review of the response process. Lessons learned from the incident will be used to improve TET's cybersecurity systems.

6. Training and Awareness

TET will conduct training sessions and awareness programs as necessary to ensure employees are familiar with this Incident Response Procedure, know how to recognize cybersecurity incidents, and understand the importance of timely reporting.

7. Plan Review and Updates

The Incident Response Procedure will be reviewed whenever significant changes occur in TET’s structure, operations, or the regulatory environment.

TASMAN
ENVIRONMENTAL TRUST

Appendix 3 | Best-practice procedures for maintaining cyber-security

1. **Use Strong and Unique Passwords**: Ensure that you use strong and unique passwords for all your online accounts. Use a combination of letters, numbers, and special characters. Consider using a reputable password manager to help you keep track of your passwords securely.
2. **Enable Two-Factor Authentication (2FA): Whenever possible, enable two-factor authentication for your accounts. This adds an extra layer of security by requiring a second form of verification in addition to your password.**
3. **Keep Software Updated: Regularly update your operating system, applications, and antivirus software. These updates often include security patches that protect your devices from known vulnerabilities.**
4. **Be Cautious with Email: Be wary of emails from unknown senders, especially those requesting personal information, financial details, or passwords. Avoid clicking on links or downloading attachments from suspicious emails.**
5. **Use Secure Wi-Fi Connections: When using public Wi-Fi networks, avoid accessing sensitive information or logging into important accounts, as these networks are often less secure. If you must use public Wi-Fi, consider using a virtual private network (VPN) to encrypt your internet connection.**
6. **Beware of Phishing: Be cautious of phishing attacks, where attackers impersonate legitimate organizations to trick you into revealing personal or financial information. Double-check URLs and verify the legitimacy of emails before clicking on links or providing information.**
7. **Secure Your Devices: Use strong PINs or passcodes to lock your devices. Enable biometric authentication if available, such as fingerprint or facial recognition.**
8. **Backup Your Data: Regularly back up important data to a secure location, such as an external hard drive or cloud storage service. This ensures you can recover your data in case of a cyber incident.**
9. **Secure Social Media Profiles: Adjust privacy settings on your social media profiles to limit the amount of personal information visible to the public. Be cautious about sharing personal details online.**
10. **Educate Yourself: Stay informed about the latest cybersecurity threats and best practices. The more you know, the better prepared you'll be to recognize and respond to potential threats.**
11. **Secure Your Home Network: If you have a home Wi-Fi network, change the default password for your router and use strong encryption (WPA3 if available). Disable remote management and regularly update the router's firmware.**
12. **Report Incidents: If you suspect a cybersecurity incident or breach, report it to your organization's IT department or relevant authorities. Prompt reporting can help mitigate the impact of an attack.**

Resources

It's important to note that cybersecurity is an evolving field, and new threats can emerge over time. Therefore TET aims to stay regularly updated on the latest security practices by being vigilant online.

For the most current guidelines specific to New Zealand: the **New Zealand Government's** CERT NZ (Computer Emergency Response Team).

Institute of Directors
Cyber risk: A practical guide 2023 | IoD NZ