Cyber Security Policy

Table of Contents

[1. Introduction 2](#_Toc141789112)

[2. Policy statement 2](#_Toc141789113)

[3. Applicability 2](#_Toc141789114)

[4. Context 2](#_Toc141789115)

[5. Responsibility of CEO, employees, volunteers, etc 2](#_Toc141789116)

[6. Levels of Confidentiality 3](#_Toc141789117)

[7. Access Control and Computers 4](#_Toc141789118)

[8. Cyber security incident response 5](#_Toc141789119)

[8.1 Prepare & Prevent 5](#_Toc141789120)

[8.2 Check and detect 5](#_Toc141789121)

[8.3 Identify and assess 5](#_Toc141789122)

[8.4 Respond 6](#_Toc141789123)

[8.5 Review 6](#_Toc141789124)

[9. Monitoring, evaluation and reporting 6](#_Toc141789125)

# Introduction

[**Name of Association**] is committed to implementing robust protective measures to effectively manage external threats that may compromise the integrity of the organisation's systems and to safeguard against potential harmful actions from external parties.

# Policy statement

This policy outlines the principles for developing, implementing, and upholding measures that safeguard the organisation's cyber assets. These assets encompass computer equipment, software, operating systems, storage media, electronic data, and network accounts. The objective is to prevent any form of exploitation or misuse that could compromise the organisation's cybersecurity.

# Applicability

This policy applies to:

* 1. All employees, contractors, volunteers and others undertaking work at [Name of Association],
	2. Visitors to the office and various workplaces or participating in authorized [Name of Association] activities including all personnel affiliated with third parties, and
	3. To all equipment owned or leased by [Organisation], and to all equipment authorised by [Organisation] for the conduct of the organisation’s business.

# Context

* 1. [Association Name] aims to provide a reasonable level of personal privacy for its users. However, it is essential for users to acknowledge that the data they generate on [Organisation]'s systems remains the property of [Organisation]. Due to the imperative need to safeguard [Organisation]'s network, the confidentiality of information stored on any network device owned by [Organisation] cannot be guaranteed. As a precautionary measure, [Organisation] reserves the right to conduct periodic audits of networks and systems to ensure compliance with this policy.
	2. Information held by the organisation will be categorized into different levels of confidentiality. Particularly sensitive information will be granted special protection.
	3. Employees and volunteers are obligated to observe all necessary cybersecurity procedures diligently. This includes safeguarding passwords, ensuring secure access to computers, and maintaining protective software.
	4. Any breach of this policy by an employee may result in disciplinary action, ranging from warnings to potential dismissal.

# Responsibility of CEO, employees, volunteers, etc

* 1. All employees have responsibility for cyber security, but specifically:

5.1.1 The CEO bears the responsibility of ensuring;

 • Staff members are informed and acquainted with this policy.

• Appropriate actions are taken to address any breaches of this policy brought to the attention of management.

• Appointment of a competent cyber security officer.

5.1.2 The cyber security officer holds the responsibility of:

• Keeping the CEO informed about any alterations in the organisation's cyber security requirements.

• Submitting an annual report on the organisation's cyber security to the board.

5.1.3 All employees and volunteers are responsible for:
• Familiarizing themselves with the cyber security policy and procedures.
• Ensuring that their use of cyber media adheres to this policy.

5.1.4 In case of any uncertainty or ambiguity regarding the requirements of the cyber security policies or procedures in a particular instance, employees and volunteers are encouraged to consult their respective supervisors.

# Levels of Confidentiality

* 1. From time to time (the Association) should issue cyber security procedures appropriate to different levels of confidentiality.
	2. The Association 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).
	3. 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 theftOrganisation data allowing banking or financial exploitation | Client credit card and banking dataOrganisational credit card and banking dataClient details that would facilitate phishing |
| Green | Client data allowing address or email exploitationOrganisational intellectual property that has financial or reputational consequences | Addresses that would facilitate spammingInformation that the organisation sellsInternal emails |
| Black | Publicly accessible data | Non-sensitive information |

# Access Control and Computers

* 1. The organisation's information resources will be allocated access based on individual clearance levels. Each person will be given access only to the resources suitable for their specific clearance. To enforce access control, username and password controls will be implemented.
	2. Users must ensure the security of their passwords. Sharing of accounts is strictly forbidden, and no other individuals should be permitted to use someone else's account. Passwords should not be kept in easily accessible areas near the respective computer. Users bear full responsibility for the security of their passwords and accounts.
	3. All workstations, PCs, and laptops are required to have a password-protected screensaver activated automatically within 10 minutes of inactivity. Alternatively, users must log off when the host device will be unattended.
	4. Every 4 months, system-level passwords must be changed, while user-level passwords should be changed at least twice per year. User accounts will be locked after three failed log-on attempts.
	5. Users who forget their password must contact [the IT department] to have a new password assigned to their account.
	6. Users are strictly prohibited from accessing password files on any network infrastructure component. Password files on servers will be continuously monitored for unauthorized access. Copying, reading, deleting, or modifying password files on any computer system is strictly prohibited.
	7. Users are not permitted to log on as system administrators. Those requiring such access must request a special password from the system administrator.

# Cyber security incident response

The CEO is responsible for an incident response plan to prepare for and respond to a cyber incident. A bi-annual scenario plan workshop should be conducted, with all staff, outlining the steps to follow should an incident occur. Steps to include:

# Prepare & Prevent

* 1. Ensure all staff follow the cyber safe policy and procedures to help employees understand how to prevent an attack and to identify potential incidents.
	2. At scenario planning identify the assets that are important to the business – financial, information and technology assets.
	3. Consider the risks to these and the steps to take to reduce the effects of an incident.
	4. Create roles and responsibilities so everyone knows who to report to if an incident occurs, and what to do next.

# Check and detect

All staff need to check and identify any unusual activities that may damage the business information and systems. Unusual activity may include:

* accounts and your network not accessible
* passwords no longer working
* data is missing or altered
* your hard drive runs out of space
* your computer keeps crashing
* your customers receive spam from your business account
* you receive numerous pop-up ads

If staff encounter a security incident, they need to document any evidence (eg take screen shots) and report it to the IT Administrator immediately.

# Identify and assess

* 1. Find the initial cause of the incident and assess the impact so you can contain it quickly.
	2. Determine the impact the incident has had on your business.
	3. Determine its effects on your business and assets if not immediately contained.

# Respond

* 1. Limit further damage of the cyber incident by isolating the affected systems. If necessary, disconnect from the network and turn off the computer to stop the threat from spreading.
	2. Remove the threat.
	3. Recover from the incident by repairing and restoring your systems to business as usual.

# Review

* 1. Identify if any systems and processes need improving and make those changes.
	2. Evaluate the incident before and after, and any lessons learnt.
	3. Update your cyber security incident response plan based on the lessons learnt so you can improve your business response.

# Monitoring, evaluation and reporting

The Chief Executive Officer is responsible for monitoring and evaluating the implementation and effectiveness of this policy and for reviewing this policy as required.

1. Last updated
	1. Approval and Review

|  |  |
| --- | --- |
| Lead Author | CEO |
| Approver | Board |
| Date endorsed |   |
| Date reviewed |   |
| Timeframe for next review | 1. months
 |

* 1. Version History

|  |  |  |
| --- | --- | --- |
|   | Date | Action |
| 1 |  Aug 2023 | Created |
| 2 |  | Approved by XX on …. |