eureka
Villages

Cybersecurity Policy

Table of Contents

Cybersecurity Policy

1. Introduction

This Cybersecurity Policy (the "Policy") outlines the measures and guidelines to be followed by all employees, contractors, and third-party vendors of Eureka Group Holdings Limited and associated subsidiaries, to protect the company's information assets from cyber threats. It is the responsibility of all individuals who access the company's systems and data to comply with this Policy to maintain the highest standards of cybersecurity.

2. Policy Objectives

The objectives of this Policy are as follows:

- Ensure the confidentiality, integrity, and availability of the company's information assets.
- Protect the company's information assets from unauthorised access, disclosure, alteration, or destruction.
- Comply with applicable laws, regulations, and industry best practices regarding cybersecurity.
- Promote a culture of awareness and accountability among employees regarding cybersecurity.

3. Scope

This Policy applies to all individuals who access, use, or manage the company's information assets, including employees, contractors, and third-party vendors. It covers all company-owned devices, systems, networks, and data, regardless of their physical location or access method.

4. Responsibilities

4.1. Management

Senior management is responsible for providing adequate resources and support to establish and maintain an effective cybersecurity program. They must ensure the implementation of appropriate security controls, regular risk assessments, and incident response procedures.

4.2. Employees

All employees are responsible for following the company's cybersecurity policies and procedures, including reporting any suspicious activities or potential security incidents promptly to their business unit senior manager who will then advise Eureka's IT provider and Incident Response Team. They must also undergo regular cybersecurity awareness training to enhance their understanding of threats and mitigation measures.

4.3. IT Managed Service Provider

The IT managed service provider is responsible for implementing and maintaining technical controls to protect the company's information assets. They must comply with the terms of the Service Level Agreement (SLA). They must monitor systems, conduct vulnerability assessments, apply patches and updates, and respond to security incidents promptly.

5. Information Classification

All information assets of the company must be classified based on their sensitivity and criticality. The company's information classification framework shall include the following categories:

- **Confidential:** Information that, if disclosed, could cause harm to the company or its stakeholders. This includes financial data, intellectual property, trade secrets, and personally identifiable information (PII).

- **Internal Use Only:** Information that is not publicly available and should be restricted to employees on a need-to-know basis. This includes internal communications, non-public financial data, and business strategies.
- **Public:** Information that is intended for public consumption and does not require any access restrictions.

6. Access Control

Access to the company's information assets must be granted based on the principle of least privilege. Employees, contractors, and third-party vendors shall only be provided with access to the systems, networks, and data necessary to perform their job responsibilities. Access rights shall be regularly reviewed and revoked promptly upon termination of employment or contract.

6.1. Endpoint Security

6.1.1. Endpoints are classified as company-owned Mobility devices (Smart Phones, Tablets), Workstations (laptops and desktops) and Servers (Physical, Virtual and/or Cloud Workloads).

- All Endpoints, where applicable, will be monitored and regularly patched by the IT provider.
- All Endpoints will have antivirus installed, monitored, and patched by the IT provider.

6.2. Network Security

6.2.1. Network devices are classified as company-owned Routers, Switches, Firewalls and Wireless Access Points & Controllers.

- All devices will be monitored and regularly patched by the IT provider.

6.3. Cloud Security

6.3.1. Cloud services may include Microsoft 365 (Email, Teams, SharePoint, and OneDrive).

- An Antispam solution will be applied to the Company email domain.
- Upgrade to M365 Business Premium - Access to all cloud services will have MFA and/or Conditional Access.

6.4. Password Requirements

6.4.1. Create Robust Passphrase - Generate strong and complex passphrases that are difficult for unauthorised individuals to guess. A strong passphrase typically consists of a combination of uppercase and lowercase letters, numbers, and special characters.

6.4.2. Proper Passphrase Storage - Safely store passphrases in a secure manner to prevent unauthorised access. Do not write them down or store them in easily accessible locations.

6.4.3. Regular Passphrase Updates - It is important to periodically update your passphrases to enhance security. Change your passphrases at least every 90 days.

6.4.4. Unique Passphrases for Each Login - Ensure that you use distinct passphrases for different accounts and logins. Avoid reusing passphrases across multiple services, as this minimises the risk of a security breach affecting multiple accounts.

6.4.5. Enable Multifactor Authentication (MFA) When Availabe - Whenever possible, activate multifactor authentication (MFA) for your accounts. MFA adds an extra layer of security by requiring you to provide two or more forms of verification before gaining access to your account, making it significantly more difficult for unauthorised access.

6.5. Guidelines for Email Usage

6.5.1. When to Share Work Email Address - Employees may share their work email address with trusted business contacts, clients, and authorised stakeholders for official communications related to their job responsibilities.

6.5.2. Email Attachments

- Only open email attachments from trusted contacts and known businesses.
- Be cautious of unexpected or suspicious attachments and verify the sender's identity before opening.

6.5.3. Blocking Junk, Spam, and Scam Emails - Employees should use email filters and report junk, spam, and scam emails to the IT provider promptly.

6.5.4. Identifying Suspicious Emails

- Be vigilant about identifying suspicious-looking emails, such as those with unexpected senders, grammatical errors, or urgent requests for sensitive information.
- Delete suspicious emails and report them to the IT provider for further investigation.

6.6. Handling Sensitive Data

6.6.1. Sensitive data refers to any information that, if compromised, could cause harm, or lead to identity theft, financial fraud, or privacy violations. Examples include:

- **Personal Information:** This includes names, addresses, contact details, dates of birth, and any other personally identifiable information (PII) that uniquely identifies our residents or employees.
- **Health and Medical Records:** Information about medical conditions, medications, and health-related history.
- **Financial Information:** Data related to bank accounts, credit card details, and financial transactions.
- **Emergency Contacts:** Contact details of emergency contacts.
- **Sharing Sensitive Data:** Employees may share sensitive data with others only when necessary for official business purposes and with proper authorisation.
- **Storing Physical Files:** Physical files containing sensitive data should be stored in locked rooms or drawers to prevent unauthorised access.
- **Identifying Sensitive Data:** Sensitive data must be properly labelled and identified to ensure appropriate handling and protection.
- **Data Destruction:** Sensitive data must be destroyed securely and permanently when it is no longer needed, following company policies and data retention.

6.7. Rules for Technology Usage

6.7.1. **Access to Devices:** Employees can access their business laptops away from the workplace when needed for work-related tasks, ensuring secure connections and compliance with data protection policies.

6.7.2. **Storing Devices:** Employees should securely store their devices, such as locking them in drawers or cabinets when not in use, to prevent unauthorised access.

6.7.3. **Reporting Device Theft or Loss:** In case of theft or loss of a work device, employees must

immediately report it to their business unit senior manager who will follow the company's incident response procedures.

6.7.4. **System Updates:** IT patches and spam filter updates will be rolled out to employee devices by the IT provider following a schedule and maintenance procedures.

6.7.5. **Shutting Down & Locking Devices:**

- Employees should physically shut down computers and mobile devices if not in use to prevent unauthorised access and conserve energy.
- Employees must lock screens when computers and devices are left unattended to prevent unauthorised access to sensitive data.

6.7.6. **Restrictions on Removable Devices:**

- The use of removable devices should be restricted to authorised personnel to prevent malware installation or data breaches.
- Data stored on removable devices should be encrypted to protect against data breaches if the device is lost or stolen.
- All removable devices must be scanned for viruses before connecting to business systems to prevent potential malware infections.

6.8. Social Media Usage

6.8.1. Appropriate Business Information on Social Media Channels - Employees must adhere to the company's social media policy when representing Eureka on social media platforms.

6.8.2. Personal Social Media Accounts

- When using personal social media accounts, employees should exercise discretion and avoid discussing confidential company matters or sharing sensitive business information.
- Employees should make it clear that their personal views and opinions expressed on personal social media accounts are their own and not representative of the company.

6.9. Guidelines for Internet Access During Work Hours

6.9.1. Appropriate Websites and Social Media Channels

- Employees should access websites and social media channels that are directly related to their job responsibilities and support their work tasks.
- Websites and social media channels that contain explicit, offensive, or inappropriate content should not be accessed during work hours.
- Personal social media usage during work hours should be limited to designated break times.

6.9.2. Compliance with Company Policies

- Employees must comply with the company's Safe and Appropriate use of Electronic Devices Policy when accessing the internet during work hours.
- Access to websites and social media channels that may pose security risks or negatively impact productivity should be avoided.

6.9.3. Prioritising Work Tasks

- Internet usage should be aligned with work priorities, and excessive personal internet browsing should be avoided during work hours.

7. Security Awareness Training

The company shall provide regular security awareness training to all employees and contractors. The training programs shall cover topics such as phishing, social engineering, password security, data handling, and incident reporting. Training materials shall be updated periodically to address emerging threats and technologies.

8. Incident Response

The company has established an incident response plan to effectively respond to and manage security incidents. The plan includes procedures for reporting incidents, containment and eradication of threats, evidence preservation, and post-incident analysis. All employees must report any suspected security incidents to the business unit senior manager promptly, who will advise the IT provider and the cybersecurity incident response team.

- The incident response team will coordinate with relevant parties, including law enforcement, regulatory authorities, and affected stakeholders, as needed.
- After an incident is resolved, a post-incident analysis will be conducted to identify lessons learned and enhance the company's security posture.

9. Compliance

The company shall comply with all applicable laws, regulations, and industry standards related to cybersecurity. This includes but is not limited to the Privacy Act, the Corporations Act, and the Australian Cybersecurity Centre's guidelines. The company shall also conduct periodic audits and assessments to ensure compliance with this Policy and make necessary improvements.

10. Policy Review

This Policy shall be reviewed periodically to ensure its effectiveness and relevance in addressing emerging cyber threats and industry best practices. Any necessary updates or amendments shall be made in consultation with the IT department and senior management.

11. Document Control Management

Policy prepared by	Natalie McGrath
Authorised by	Board
Date issued	October 2023
Frequency of reviews	Biennial
Next review date	October 2025