CYBERSECURITY POLICY - TEMPLATE

Instructions

On company letterhead and signed by the appropriate officer.

We recommend members consider the template carefully prior to implementation in your business. It contains content that may require customisation. Given the nature of the subject this policy will need to suit your particular business and its needs.

We recommend members periodically review and update this policy.

Communicate this policy and any changes with your employees.

This policy should be read in conjunction, and applied with, any other relevantly applicable company policies.

Remove all instructions and other VMA related references prior to implementation in your business.

Seek advice from VMA should related issues arise in the workplace.

This policy provides guidelines to protect [*insert business name*]'s digital systems, data, and communications.

This policy aims to balance the following priorities:

i. Meeting our legislative requirements
ii. Keeping data and documents confidential as required by the company, its customers, and stakeholders
iii. Ensuring the integrity of the company's data and IT systems
iv. To uphold the company's reputation as a trusted recipient of data
v. Maintain storage and back-up systems that meet the needs of the company

This policy applies to all employees, contractors, vendors and anyone else who may have any type of access to the company's systems, software, hardware, data and or documents.

Cyber Risks Include:

- Financial loss
- Operational disruption
- Legal or reputational damage
- Privacy breaches

Examples of Threats

There are a range of potential cyber and data related threats the company face. These include:

- **Malware** – harmful software
- **Ransomware** – blocking access to files, systems or networks unless money is paid
- **Phishing** – fraudulent messages
- **Man-in-the-middle** – intercepted communications
- **Denial-of-Service** – disabling systems
- **Supply Chain Attacks** – targeting suppliers or clients to compromise their systems and gain access to a target organisations network

---

Employee Responsibilities

All employees must:

- Exercise caution when sharing information and documents, giving access to information systems, and when authorising any individual to enter and control systems.
- Attend cyber security training where directed.
- Use strong, unique passwords and Multi Factor Authentication tools where possible.
- Avoid opening suspicious emails and links.
- Block junk, spam and scam emails.
- Do not write down passwords or otherwise leave any password unprotected.
- Change passwords where there is a possibility of it having been compromised, and otherwise change passwords on a six monthly basis.
- Not install unauthorised software and apps. The company may at any time introduce a whitelist of approved/trusted programs and apps. Only those programs and apps may be used.
- Only share data over authorised networks.
- Perform appropriate protocols and procedures are followed to backup and store information.
- Not attempt to circumvent or turn off any security related measures.
- Secure devices and shred sensitive hardcopy material that is no longer required.
- When working remotely, all cybersecurity and data protocols and procedures must be followed. This includes ensuring devise have current antivirus software, and that all company data is stored on approved storage platforms.
- Ensure company information does not remain on hardware that becomes obsolete.
- Immediately report to their manager and or IT department any security concerns, breaches, suspicious activity or issues that may cause a cybersecurity breach.

Prohibited Conduct

- Sharing confidential or sensitive data with unauthorised people
- Purposefully engage in any activity that degrades the performance of any system
- Gain access to any system for which you do not have authorisation

- Making unauthorised copies of any confidential or sensitive information and or distribute it outside the company
- Circumvent or turn off any security related measures
- Using personal and work accounts interchangeably
- Leaving devices unlocked or unattended
- Clicking on suspicious links or offers

Non-compliance with this policy may lead to disciplinary action.

Policy Review

The company will periodically review this policy and update as required to ensure the continued security of the company, its clients, and stakeholders.

This policy commences on [*insert date*].

……
Position: [Signed by appropriate officer]
Date: [insert date]
Next review date: [*insert next review date*]

Support and Further Information

For assistance, please contact the Visual Media Association HR/IR Advisory Service:

P: 1800 835 167

E: hrhelp@visualmediaassociation.org.au