## IT SECURITY AND CYBERSECURITY POLICY AND PROCEDURES

### Purpose

The purpose of this IT Security and Cybersecurity Policy is to establish a framework for protecting Trendie's information systems, data, and networks from security threats and unauthorised access. This policy aims to safeguard the confidentiality, integrity, and availability of our digital assets and ensure compliance with relevant Australian laws and regulations. It provides clear guidelines and procedures for all employees to follow, ensuring that Trendie's IT infrastructure is secure and resilient against cyber threats.

### Scope

This policy applies to all employees, contractors, and third parties who have access to Trendie's information systems and data. It covers all forms of digital information, including but not limited to emails, databases, cloud services, hardware, software, and network resources. This policy is applicable to all devices used to access company systems, whether owned by Trendie or by the individual.

### Relevant Australian Legislation and Regulations

- **Privacy Act 1988 (Cth):**

  Ensures the protection of personal information handled by organisations.

- **Australian Privacy Principles (APPs):**

  A set of guidelines that govern the handling of personal information.

- **Notifiable Data Breaches (NDB) Scheme:**

  Mandates the reporting of data breaches that are likely to result in serious harm.

- **Australian Cyber Security Centre (ACSC) Guidelines:**

  Provides best practice recommendations for cybersecurity measures.

- **Crimes Act 1914:**

  Addresses offences related to unauthorised access, modification, or impairment of data.

## Policy Principles

- **Confidentiality:**

  Employees must ensure that all sensitive information, including personal, financial, and proprietary data, is kept confidential and only accessible to authorised individuals. Unauthorised disclosure of confidential information is strictly prohibited.

- **Integrity:**

  All employees are responsible for maintaining the accuracy and reliability of Trendie’s data. Alterations to data must be authorised and documented to ensure data integrity.

- **Availability:**

  IT systems and data must be available to authorised users when needed. Employees must report any issues or disruptions that could affect the availability of these systems.

- **User Access Management:**

  Access to company systems and data is granted based on the principle of least privilege, where users are given the minimum access necessary to perform their duties. Access rights must be reviewed and adjusted regularly to reflect changes in job responsibilities.

- **Use of Company Systems:**

  Employees must use company-provided systems, software, and networks for authorised business purposes only. Personal use of these resources should be minimal and must not compromise security.

- **Incident Response:**

  Employees must report any suspected or actual security incidents immediately. Prompt reporting enables Trendie to take swift action to mitigate potential damage.

- **Compliance and Training:**

  All employees must comply with this policy and participate in regular cybersecurity training to stay informed about the latest threats and best practices.

**Procedures**

- **User Access Management Procedures:**
    - **Account Creation and Deletion:** User accounts will be created by the IT department upon authorisation from HR. Access rights will be determined based on the employee's role. Upon termination or change in role, accounts will be promptly updated or deactivated.
    - **Password Policy:** All employees must use strong, unique passwords for accessing company systems. Passwords should be at least 12 characters long and include a mix of letters, numbers, and symbols. Passwords must be changed every 90 days and should not be reused across different systems.
    - **Multi-Factor Authentication (MFA):** MFA is mandatory for accessing critical systems and data. Employees must use an additional verification method, such as a mobile app or hardware token, in conjunction with their password.
- **Data Protection Procedures:**
    - **Data Encryption:** All sensitive data must be encrypted both in transit and at rest. This includes emails, files, and database records. The IT department is responsible for ensuring that encryption protocols are properly implemented.
    - **Data Backup:** Regular data backups must be performed to ensure business continuity in the event of a data loss incident. Backups should be stored in a secure, off-site location and tested regularly for integrity.
    - **Data Retention and Disposal:** Personal and business data must be retained in accordance with the company's data retention policy and relevant legislation. Data no longer required must be securely disposed of using methods such as shredding or secure digital erasure.
- **Use of Company Systems Procedures:**
    - **Acceptable Use:** Employees are expected to use company systems responsibly and in accordance with this policy. The use of company systems for illegal, unethical, or unauthorised activities is strictly prohibited.
    - **Software Installation and Updates:** Only authorised software should be installed on company devices. The IT department will manage software updates to ensure systems are protected against vulnerabilities.

  - **Remote Access:** Employees accessing company systems remotely must use secure methods, such as VPNs, to protect data in transit. Remote access should be limited to essential business needs.

- **Incident Response Procedures:**
  - **Reporting:** Employees must report any security incidents, including phishing attempts, malware infections, or unauthorised access, to the IT department immediately. Reports can be made via email or the company's incident reporting system.
  - **Investigation and Response:** The IT department will investigate reported incidents promptly and take appropriate action to contain and mitigate the threat. This may involve isolating affected systems, removing malware, or notifying affected individuals.
  - **Notification:** In the event of a data breach that may cause serious harm, Trendie will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) in accordance with the Notifiable Data Breaches (NDB) scheme.
- **Compliance and Training Procedures:**
  - **Employee Training:** All employees must complete cybersecurity awareness training upon joining the company and participate in regular refresher sessions. Training will cover topics such as recognising phishing attempts, safe internet practices, and incident reporting procedures.
  - **Policy Review and Updates:** This policy will be reviewed annually to ensure it remains effective and complies with current legislation and best practices. Any updates will be communicated to all employees.

### Compliance and Enforcement

Trendie is committed to enforcing this IT Security and Cybersecurity Policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Employees found responsible for security breaches or misuse of company systems may also be subject to legal action under relevant Australian laws.

### Review and Updates

This policy will be reviewed and updated annually, or as required by changes in legislation, regulations, or organisational needs. Employees will be informed of any changes and are expected to familiarise themselves with the updated policy.

### Implementation

The IT department will oversee the implementation of this policy, providing necessary resources, training, and support to ensure compliance. Employees will be required to acknowledge their understanding of and commitment to this policy as part of their onboarding process.

By adhering to this policy, employees help protect Trendie's digital assets, maintain the trust of our clients, and ensure the ongoing security and integrity of our information systems.