[INSERT COMPANY HEADER]

(the "Company")

Cyber Security Policy (Template)

---

1. Policy Brief & Purpose

The cyber security policy outlines the organisation's guidelines and provisions for preserving the security of our data and technology infrastructure. The more technology is relied on to collect, store, and manage information, the more vulnerable the organisation is to severe security breaches. Human errors, hacker attacks, and system malfunctions could cause great financial damage and may jeopardize our organisation's reputation. For this reason, a number of security measures have been implemented and instructions have been prepared to help mitigate security risks. Both provisions are outlined in this policy.

---

2. Scope

This policy applies to all the organisation's staff, contractors, interns, and anyone who has permanent or temporary access to the organisation's systems and hardware.

---

3. Policy Elements

Confidential Data

- Confidential data is secret and valuable. Common examples are:
  - Unpublished financial information
  - Data of customers/partners/vendors
  - Customer lists (existing and prospective)
- All staff are obliged to protect this data.

---

4. Protect Personal and Organisation Devices

- When staff use their digital devices to access organisation's emails or accounts, they introduce security risk to our data. They can do this if they:
  - Keep all devices password protected.
  - Choose and upgrade a complete antivirus software.
  - Ensure they do not leave their devices exposed or unattended.
  - Install security updates of browsers and systems monthly or as soon as updates are available.
  - Log into the organisation's accounts and systems through secure and private networks only.
- Staff should avoid accessing internal systems and accounts from other people's devices and / or lending their own devices to others.

---

5. Data Transfer

- Staff should ensure the security of data when transferring it. This includes:
  - using encrypted communication channels;
  - avoiding sharing sensitive information over unsecured networks;
  - following the organisation's guidelines for data transfer.

---

6. **Reporting Mechanisms**
    - Staff should report any scams, privacy breaches, and potential security threats immediately to the IT department or their Manager;
    - The organisation will ensure timely response and resolution of reported issues.

---

7. **Disciplinary Action**

In accordance with the organisation's Disciplinary Policy, violations of this policy may result in disciplinary action, up to and including termination of employment.

---

8. **Responsibilities**
    - **IT Department**: Responsible for implementing and maintaining security measures.
    - **Staff**: Responsible for adhering to the security guidelines and reporting any security incidents.

---

9. **Review and Updates**

This policy will be reviewed annually and updated as necessary to ensure it remains relevant and effective.
