**Cyber Security Policy Template**

**Cyber Security Policy**
*Effective Date:* [Date]
*Last Reviewed:* [Date]

**1. Purpose**
This policy outlines the cyber security practices and responsibilities to protect the organisation’s information, systems, and networks from cyber threats.

**2. Scope**
This policy applies to all employees, contractors, vendors, and any third parties with access to the organisation's information and systems.

**3. Roles and Responsibilities**

* **Business Owner / IT Administrator**: Ensures overall security of systems, implements security measures, and oversees compliance with the policy.
* **Employees**: Follow security protocols, report incidents, and maintain good security practices.

**4. Access Control**

* Access to systems and data is restricted to authorised personnel only.
* Passwords must be strong, unique, and changed every [90 days]. Two-factor authentication (2FA) is required for critical systems.

**5. Data Protection**

* All sensitive data must be stored securely, using encryption when applicable.
* Regular backups of important data are to be performed and stored securely offsite or on a cloud-based solution.

**6. Device Security**

* All devices must be protected with antivirus software and updated regularly.
* Employees are prohibited from installing unauthorised software on company devices.
* Lost or stolen devices must be reported immediately to the IT Administrator.

**7. Network Security**

* A firewall must be used to protect the business network.
* Public Wi-Fi networks are not to be used for accessing sensitive information or systems.
* Remote access to the company network requires a secure VPN connection.

**8. Incident Response**

* Any suspected or actual security incident (e.g., data breach, malware infection) must be reported immediately to the IT Administrator.
* An incident response plan will be followed to contain, investigate, and resolve security incidents.

**9. Email and Internet Usage**

* Avoid clicking on unknown links or downloading attachments from unknown sources.
* Business email should only be used for work-related communications.
* Employees should not use personal accounts for business communications.

**10. Employee Training**

* Cyber security awareness training will be conducted at least once per year.
* Employees will be trained to recognise phishing emails, social engineering tactics, and other common threats.

**11. Policy Review**

* This policy will be reviewed annually or in response to a security incident.
* Updates to the policy will be communicated to all employees.

**12. Compliance**

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or business relationship.

**Acknowledgment of Policy**

*I have read, understood, and agree to adhere to the Cyber Security Policy.*

Employee Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***This simple cyber security policy template will help your businesses secure your data and systems. It can be customised further based on the specific needs of your business.***