

CYBER SECURITY POLICY

Effective	Date	
Reviewed by	The	
next scheduled review date		
Supersedes	All previous similar policies	
Approved by		
Date Approved		

1 Purpose

The purpose of this Cyber Security Policy is to outline the necessary practices, roles, and guidelines for protecting our organisation's information assets, systems, and networks from potential cyber threats. This policy aims to safeguard data integrity, availability, and confidentiality while minimising risks associated with cybersecurity breaches.

1.2 Scope

This policy applies to all employees, contractors, vendors, and any parties accessing or managing the organisation's systems, data, or networks. It covers all types of data, including personal, financial, operational, and intellectual property, as well as any hardware, software, and network systems.

2.0 Cyber Security Policy

2.1. Access Control and Authentication

To ensure that only authorised personnel access sensitive data and systems, the following protocols must be enforced:

- ❑ **User Authentication:** All users must use strong passwords, adhering to the company's Password Policy. Multi-Factor Authentication (MFA) is required for accessing critical systems.
- ❑ **Access Privileges:** Access will follow the principle of least privilege. Employees receive access only to systems and data necessary for their job functions.
- ❑ **Regular Audits:** Access permissions will be reviewed quarterly, with updates as required by role changes or employment status.

2.2. Data Protection and Confidentiality

Data protection is critical to maintaining customer trust and compliance with regulatory standards.

- ❑ **Data Encryption:** Sensitive data, both in transit and at rest, must be encrypted using industry-standard encryption protocols.

Data Classification: All data will be classified (e.g., Confidential, Internal, Public), with handling procedures in place for each classification level.

- **Data Disposal:** Data that is no longer needed must be disposed of securely, following the company's Data Disposal Policy.

2.3. Device and Network Security

To protect the organisation's network from unauthorised access and cyber threats:

- **Firewall and Antivirus Software:** All network traffic will be monitored through firewalls, and up-to-date antivirus software must be installed on all devices connected to the network. **Patch Management:** Regular software and hardware updates, including patches, must be applied promptly to prevent vulnerabilities. **Remote Access Security:** Remote connections must utilise secure protocols, such as VPN, and adhere to the Remote Access Policy.

2.4. Incident Response and Reporting

A structured approach to responding to and reporting cybersecurity incidents is essential for minimising damage.

- **Incident Detection and Response:** A Cybersecurity Incident Response Team (CSIRT) will manage incident detection and response. Employees must report any suspicious activities or security incidents immediately.
- **Incident Reporting:** All incidents, including potential phishing, malware infections, or data breaches, should be documented in the incident log.
- **Root Cause Analysis:** For significant incidents, a root cause analysis will be conducted to identify vulnerabilities and prevent future occurrences.

2.5. Security Awareness and Training

Regular training helps employees stay informed on best practices and recognise potential threats.

- **Mandatory Cybersecurity Training:** All employees must complete cybersecurity training annually, covering topics like phishing, password management, and safe internet usage.
- **Simulated Phishing Tests:** Regular phishing simulations will be conducted to assess and enhance employee awareness.
- **Continuous Learning:** Employees are encouraged to participate in additional cybersecurity workshops and courses to stay updated on evolving threats.

2.6. Third-Party and Vendor Security

Vendors and third parties that access or manage our systems or data must comply with cybersecurity standards.

- **Vendor Screening:** Prior to engagement, all vendors will undergo a security risk assessment to ensure they meet our cybersecurity requirements.
- **Contractual Obligations:** Vendor agreements must include cybersecurity compliance clauses, ensuring adherence to our security policies and data protection laws.
- **Ongoing Monitoring:** The organisation will monitor vendor access and security practices to ensure continuous compliance.

2.7. Network Monitoring and Threat Detection

Network and system monitoring is critical to detect and respond to unusual activities.

- ❑ **Real-Time Monitoring:** Continuous network monitoring and intrusion detection systems (IDS) will identify and alert on any suspicious activities.
- ❑ **Log Management:** All system and application logs will be securely stored and regularly reviewed by authorised personnel.
- ❑ **Threat Intelligence:** The organisation will use threat intelligence feeds to stay aware of new cybersecurity threats and adjust defences accordingly.

2.8. Compliance and Regulatory Adherence

To avoid legal repercussions and ensure customer trust, the organisation must comply with all relevant cybersecurity regulations.

- ❑ **Regulatory Compliance:** The organisation must comply with regulations like GDPR, HIPAA, and any industry-specific cybersecurity mandates.
- ❑ **Policy Reviews:** This policy will be reviewed and updated annually to reflect changes in regulations, standards, or threats.
- ❑ **Documentation:** All compliance activities, including training records and audit logs, must be documented and retained for regulatory reviews.

3.0 Policy Compliance

3.1 Compliance Measurement

The Information Security team will regularly audit and monitor compliance with this policy, using reports, assessments, and performance indicators.

3.2 Exceptions

Any exception to this policy must be formally approved by the Information Security Officer after a risk assessment.

3.3 Non-Compliance

Violations of this policy may result in disciplinary action, up to and including termination of employment, and, if necessary, legal action.

This Cyber Security Policy is essential for creating a robust cybersecurity posture, protecting organisational assets, and fostering a culture of security awareness across the organisation. Regular training, monitoring, and policy updates will be crucial in adapting to evolving threats and maintaining a proactive defence.