Cyber Policy and Procedures

DISTRIBUTION

This Cyber Policy & Procedures is communicated to all employees. A copy is available at the Head Office, held in the sites folder, and published on the internal company shared drive. All employees are encouraged to read it and communicate any queries to a Director.

REVISION HISTORY

Issue Number	Review Date	Changes	Signed
01	22/09/2023	Original version (draft)	
01	22/09/2023	Signed off	
01	20/09/2024	Review	
01	19/09/2025	Review	
02	20/05/2026	Address Updated	
02	18/09/2026	Review	

Password Management:

All employees must create strong passwords and keep them confidential.

- Employees must not reuse passwords across different accounts or systems.
- Employees must change their passwords every 90 days.
- Employees must not share their passwords with anyone, including colleagues or IT staff.

Network Security:

- Employees must not connect unauthorized devices (such as personal laptops, smartphones, or USB drives) to the company network.

- Employees must not download or install any software on company devices without approval from IT.
- Employees must not access any malicious or suspicious websites while using company devices.
- Employees must report any security incidents (such as suspicious emails or malware) to IT immediately.

Email Security:

- Employees must be cautious when opening emails from unknown senders.
- Employees must not click on any links or download attachments from suspicious emails.
- Employees must not provide personal or sensitive information (such as passwords or financial information) via email.

Data Protection:

- Employees must handle all company data with care and protect it from unauthorized access or disclosure.
- Employees must not share company data with unauthorized individuals.
- Employees must report any data breaches or accidental data disclosures to IT immediately.

Mobile Device Security:

- Employees must password-protect their company-issued mobile devices.
- Employees must not connect to unsecured wireless networks while using company devices.
- Employees must report any lost or stolen company devices to IT immediately.

Physical Security:

- Employees must secure company devices and facilities when not in use.
- Employees must report any security breaches or attempts to access company devices or facilities to IT immediately.

User Responsibilities:

- Employees must adhere to all cyber policy and procedures outlined in this document.
- Employees must report any violations of this policy to IT immediately.
- Employees must complete regular cyber security training to stay up-to-date on the latest threats and best practices.

Cyber Policy and Procedures

Access Control:

- Employees must only access systems and data that they have been authorized to use.
- Employees must log out of all systems when they are not in use.
- Employees must not attempt to bypass security controls or access restricted areas.

Network Access:

- Employees must use the company's virtual private network (VPN) when accessing the network remotely.
- Employees must not use public Wi-Fi networks to access the company network.
- Employees must use strong passwords and two-factor authentication when accessing the company network remotely.

Data Backup:

- The company will regularly back up important data to ensure it can be recovered in the event of a disaster.
- Employees must not store company data on personal devices or cloud storage services without approval from IT.
- Employees must report any data loss or corruption to IT immediately.

Vendor Security:

- The company will only work with vendors that demonstrate strong cyber security practices.
- Employees must follow all vendor security guidelines when working with company data.
- Employees must report any security concerns with vendors to IT immediately.

Incident Response:

- The company will have an incident response plan in place to address cyber security incidents.
- Employees must follow the incident response plan in the event of a cyber-security incident.
- Employees must report any cyber security incidents to IT immediately.

Compliance:

- The company will adhere to all relevant cyber security laws and regulations.

Cyber Policy and Procedures

- Employees must comply with all relevant cyber security laws and regulations when handling company data.
- Employees must report any compliance concerns to IT immediately.

Managing Director

Name: Danish Iftikhar

Sign: 

Dated: 22/09/2023