Cyber Security Policy

Version Control

Version	Date	Author	Reason for revision
V1	06/2023	FRWRD IT	Document Creation

Disclaimer

This policy has been developed to ensure the safe, efficient, and lawful use of the organisation's cyber and information resources. It aims to protect our employees, partners, the organisation, and our customers from harm caused by both deliberate and inadvertent misuse of our digital assets, data, and systems.

Purpose

The purpose of this policy is to define the rules and standards for the use of our organisation's cyber resources, including but not limited to information systems, hardware, software, networks, and data. It is designed to guide users in understanding what behaviour is considered acceptable and what behaviour is considered unacceptable.

Asset Management

1.1. All digital assets, including but not limited to hardware, software, and information, shall be catalogued in a secure and organised manner.

1.2. The company shall maintain an updated register of all digital assets, complete with their specific characteristics, values, and ownership details.

1.3. Regular audits will be conducted to verify the location, condition, and usage of each asset.

Risk Management

2.1. A comprehensive risk management approach shall be used to identify, analyse, evaluate, and treat potential risks.

2.2. Risk assessments shall be carried out on a regular basis to identify any vulnerabilities that may be exploited by cyber threats.

2.3. Appropriate measures will be implemented to mitigate identified risks.

Identity Management and Access Control

3.1. User access to company systems shall be strictly controlled and monitored.

3.2. Strong, unique passwords and two-factor authentication (2FA) are required for all users.

3.3. Access privileges will be based on a user's role and responsibilities.

Data Security

4.1. Data shall be classified into appropriate levels of sensitivity and handled accordingly.

4.2. All data shall be encrypted during transmission and stored securely at rest.

4.3. Periodic backups of critical data shall be made and stored in a secure location.

Threats to Assets

The identified threats to the technology and information assets include, but are not limited to:

• Unauthorised access and data breaches

• Malware, viruses, and ransomware attacks

• Phishing and social engineering attempts

• Physical theft or loss of devices

• Insider threats and unauthorised use

Acceptable Use of Devices and Online Materials

• Employees should use company-provided devices for work purposes only.

• Personal use of devices should be limited to designated break times.

• Accessing inappropriate websites, downloading unauthorised software, or engaging in illegal activities is strictly prohibited.

Handling and Storage of Sensitive Material

• Physical files containing sensitive data should be stored in locked cabinets or rooms accessible only to authorized personnel.

• Digital sensitive data should be encrypted and stored in secure, password-protected locations.

• Sensitive material should never be left unattended in public areas.

Password Requirements and Best Practices

• All users must create strong passphrases that are at least 12 characters long, including a mix of uppercase and lowercase letters, numbers, and special characters.

• Passphrases should not be easily guessable, such as using personal information or common dictionary words.

• Passphrases must be stored securely, using password management tools or encrypted storage methods.

• Passphrases should be changed every 90 days or immediately if there is suspicion of compromise.

• Employees must use unique passphrases for different logins to prevent credential reuse.

Email Security Measures

• Work email addresses should only be shared with trusted contacts and for legitimate business purposes.

• Employees should exercise caution when opening email attachments, verifying their authenticity before accessing them.

• Junk, spam, and scam emails should be immediately deleted and reported to the IT department.

• Employees should be trained to identify and report suspicious-looking emails that may be phishing attempts or contain malware.

Handling of Sensitive Data

• Staff may only share sensitive data with others on a need-to-know basis and with appropriate authorization.

• Physical files with sensitive data must be labeled as such and stored securely when not in use.

• Sensitive data should be properly identified through classification and labeling mechanisms.

• When sensitive data is no longer needed, it should be destroyed using secure deletion methods or through shredding physical documents.

Rules for Handling Technology

• Employees may access business devices, such as laptops, away from the workplace when required for work purposes.

• Devices should be stored securely when not in use, such as in locked drawers or cabinets.

• The loss or theft of a work device must be immediately reported to the IT department and management.

• System updates, patches, and spam filter updates will be rolled out by the IT department to employee devices.

• Computers and mobile devices must be physically shut down when not in use for an extended period.

• Screens must be locked when computers and devices are left unattended.

• USB sticks and other removable devices should only be used after scanning for viruses and malware.

• The use of removable devices is restricted to prevent unauthorized installation of malware on company systems.

Standards for Social Media and Internet Access

• Employees should be cautious about sharing appropriate business information on social media channels.

• Work email accounts should only be used for business-related communication and not for personal use.

• Guidelines will be provided on accessing appropriate websites and social media channels during work hours, ensuring productivity and security.

Incident Response

In the event of a cyber security incident, the following steps should be followed:

• Respond promptly to the incident, following predefined incident response procedures.

• Notify the IT department and relevant management personnel immediately.

• Identify the incident's cause, contain it to prevent further damage, and restore systems to normal operation.

• All employees should be aware of their roles and responsibilities during a cyber attack.

• After the incident, conduct a thorough review to identify any system or process improvements and update the incident response plan accordingly.

Incident Response Plan

An incident response plan will be developed and implemented to ensure a swift and effective response to cyber incidents. The plan will cover the following stages:

6.1 Prepare and Prevent

• Educate employees about cyber security best practices and the prevention of cyber attacks.

• Identify and prioritise important assets and implement measures to reduce risks.

• Establish clear roles and responsibilities for incident response team members.

6.2 Check and Detect

• Regularly monitor systems for any unusual activities or signs of compromise.

• Implement intrusion detection systems and security event monitoring tools to identify potential incidents.

6.3 Identify and Assess

• Investigate and determine the cause and impact of the incident.

• Assess the potential effects on business operations and assets.

6.4 Respond

• Isolate affected systems to limit further damage.

• Remove the threat and restore affected systems.

• Implement recovery procedures to return to normal business operations.

6.5 Review

• Evaluate the incident response process and identify areas for improvement.

• Update the incident response plan based on lessons learned to enhance future response capabilities.

Acceptable Use of Social Media and Other Public Technologies

6.1. Any company-related communication on social media or public platforms must be approved by the management.

6.2. Employees must not share sensitive or proprietary information on these platforms.

6.3. Personal use of social media during work hours should be limited and should not interfere with duties.

Rules and Guidance around Homeworking

7.1. Employees working remotely must follow the same cybersecurity protocols as in-office employees.

7.2. Company data must not be stored or transmitted on personal devices unless those devices meet company security standards.

7.3. Video conferencing platforms must be secure and approved by the IT department.

Data Protection

8.1. The company shall adhere to all local and international data protection laws.

8.2. Personal data shall only be collected, stored, and processed with explicit consent.

8.3. Data breaches must be reported promptly to both affected parties and regulatory authorities.

Please note that this policy does not supecede any Data Protection or GDPR Policy within the company

Computer Misuse

9.1. Unauthorized access, alteration, or destruction of company resources is strictly prohibited.

9.2. Any suspected misuse should be immediately reported to the IT department.

9.3. Misuse can result in disciplinary action, up to and including termination and legal action.

Computer & Network Security

10.1. Firewall and antivirus software shall be maintained on all company systems.

10.2. Regular security audits will be performed to identify and rectify vulnerabilities.

10.3. Wireless networks must be encrypted and access controlled.

10.4 Computer Security is everyone's responsibility - if you see an unlocked and unattended computer - lock it.

Limitations to What Data Can Be Accessed on Work Devices

11.1. Access to data will be limited to job responsibilities.

11.2. Personal use of work devices should be limited and should not include activities that put company data at risk.

11.3. Access to non-work related websites or services can be restricted at the discretion of the IT department.

Compliance with this policy is mandatory for all employees, and violations may lead to disciplinary action. This policy is subject to periodic review and updates.

By adhering to this Cyber Security Policy, all employees and contractors contribute to maintaining a secure and resilient digital environment for the Construction Recruitment Company.