Construction Square Ltd

Cybersecurity Policy

Version: 1.1

Date: 27/11/2025

Policy Change Log		
Version	**Date**	**Summary of Changes**
1.0	22/01/2025	First issue
1.1	27/11/2025	Branding Update, following rebranding from Cold Square to Construction Square

CONSTRUCTION SQUARE

1. Purpose

The purpose of this Cybersecurity Policy is to safeguard the assets, data, and reputation of Construction Square Ltd. by establishing robust cybersecurity practices. This policy aligns with the principles of the Cyber Essentials Toolkit (UK) and aims to protect the business against cyber threats, ensure compliance with relevant regulations, and build trust with our clients and stakeholders.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals with access to Construction Square Ltd.'s systems, devices, or data. It covers all company-owned and personal devices used for business purposes, networks, software, and any data related to company operations.

3. Roles and Responsibilities

- **Company Management:** Responsible for approving and enforcing this policy, providing resources for implementation, and ensuring compliance.
- **IT Administrator:** Responsible for maintaining and monitoring systems, implementing cybersecurity measures, and responding to incidents.
- **Employees:** Responsible for adhering to this policy, reporting potential threats, and maintaining good cyber hygiene practices.
- **Third Parties:** Required to comply with this policy when accessing or using company systems or data.

4. Acceptable Use of Technology

- Company devices and systems must be used solely for authorised business purposes.
- Employees must not install unauthorised software or applications on company devices.
- Access to social media, streaming, or non-work-related websites should be limited and only as permitted by management.

5. Data Security Measures

- **Access Control:** Access to sensitive data and systems will be restricted based on job roles and responsibilities. Strong authentication methods, such as two-factor authentication (2FA), will be implemented.
- **Data Encryption:** All sensitive data stored on devices or transmitted over networks must be encrypted.
- **Data Backup:** Regular backups of critical data will be performed and securely stored in line with disaster recovery procedures.

6. Cyber Hygiene Practices

- **Passwords:** Employees must use strong, unique passwords. If a password is suspected to be compromised, it must be changed immediately. Passwords should be reviewed periodically (e.g., every 90 days) to ensure they remain secure.
- **Software Updates:** All devices must have the latest security patches and updates installed promptly.

- **Antivirus Protection:** All company devices must have approved antivirus software installed and running at all times.
- **Email Security:** Employees must be vigilant for phishing emails and avoid clicking on links or downloading attachments from unknown sources.

7. Incident Response Plan

- Employees must immediately report any suspected security incidents, such as phishing attempts, ransomware attacks, or data breaches, to the IT Administrator.
- The IT Administrator will assess and respond to incidents, isolating affected systems and notifying stakeholders if necessary.
- Incidents will be documented, and steps will be taken to prevent recurrence.

8. Training and Awareness

- All employees will receive regular cybersecurity training to recognize common threats and understand their responsibilities.
- Training sessions will include topics such as phishing, password security, and secure data handling.

9. Third-Party and Vendor Management

- Vendors and contractors are expected to align with this policy and may be asked to sign a cybersecurity agreement before accessing company systems or data.
- Regular audits of third-party access will be conducted to ensure compliance.

10. Monitoring and Review

- The IT Administrator will monitor systems and networks for suspicious activity and potential vulnerabilities.
- This policy will be reviewed annually or after significant incidents to ensure it remains effective and up to date.

11. Compliance and Enforcement

- Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contracts.
- Serious breaches may be reported to legal authorities as required.

Acknowledgment All employees, contractors, and vendors must read and acknowledge this policy to confirm their understanding and commitment to compliance.

Parsa Jomehpour Arashlou

Director
Construction Square Ltd

Parsa Jomehpour Arashlou
Parsa Jomehpour Arashlou (Nov 27, 2025 18:38:54 GMT)