IT POLICY

Revised and updated March 2024

SigmaRoc is an AIM-quoted lime and limestone group targeting quarried materials assets in the UK and Northern Europe.

SigmaRoc aims to ensure that our business activities are carried out in a manner that ensures the protection of IT systems and data.

We aim to ensure that our employees are aware of their responsibilities for the leadership, resourcing, implementation, compliance and monitoring of systems and data within their control and work proactively to ensure that all risk is controlled though effective process and employee engagement.
The core areas that will enable us to achieve our vision are:

1. **People and Systems Usage**

There will be:

A Data Protection Officer (DPO), where required, or someone in charge of Information Security.
Controls to ensure timely removal of system access when an employee leaves the organisation, or when access is no longer required for business purposes.
Policy governing security, privacy and acceptable use of company systems and property that must be followed by anyone who accesses your network or sensitive information in your care.

Annual training in privacy and security related matters such as phishing, use of social media and mobile devices.
Policies and procedures regarding systems, internet, email and social media usage including downloading and installation of third-party applications.

Continual monitoring and recording of businesses systems, business and user data for compliance, training and security purposes.

2. **Impersonation Fraud**

There will be:

Control and validation of accepting fund transfer instructions
Anti-fraud training including but not limited to detection of impersonation fraud or phishing scams.
Independent verification of request to pay / transfer funds made by an employee.
Independent verification of request to change payment details by external parties.

3. **Data Protection**

There will be:

Knowledge and security of sensitive or private information and ability to contact individuals if their information is breached.

A Board approved policy that addresses compliance with privacy and security laws / regulations.
Website privacy policy.

4. System Security & remote Access

There will be:

Physical security measures for access to datacentres / server rooms.
Data retention & destruction as per local legal requirements and recommended best practices.
Controlled asset disposals to ensure recycling and data protection.
External network integrity assessments and timely close out of actions.
Up to date security in place such as firewalls and anti-virus as per software providers recommendations.
Endpoint protection, database encryption, intrusion prevention, detection or data loss prevention software deployed.
Changes to default settings to ensure information security systems, including network connected telephone systems, are securely configured.
Remote access control using two-factor authentication.
Password/account log in.
Daily / weekly backups of data, applications and system configurations that are encrypted and securely stored.
Cloud-based systems accessible via 4G dongles and regular back-ups, with offline manual functions available to assist in business continuity
Disabling, where not needed, of data transfer via USB ports.

Encryption of all sensitive data that is physically removed from your premises by mobile device e.g. laptop, mobile/ portable devices.

5. Payment Card Industry & Data Security Standard

There will be:

PCI compliance by the businesses of outsourced provider to the appropriate level.
Changes of default usernames and passwords for payment systems.
Process and procedure for deploying patches to point of sale devices.
Network segmentation used to isolate PCI information from the rest of the corporate network.

6. Vendor Management

Where services are outsourced, each business will ensure that the software and the service providers such as those listed below are competent and compliant to the best of their abilities to this policy:

- Main Provider
- Billing or Payment Service
- Back-up & Data Recovery
- Hosting
- Internet Service Provider (ISP)
- Payment Processor
- Managed Security Service

SigmaRoc are committed to ensuring that all our activities are managed in a way that minimises risk and prevents negative impact to our IT Systems and Data.

This Policy will be reviewed periodically by the board to ensure it meets the needs of the organisation.