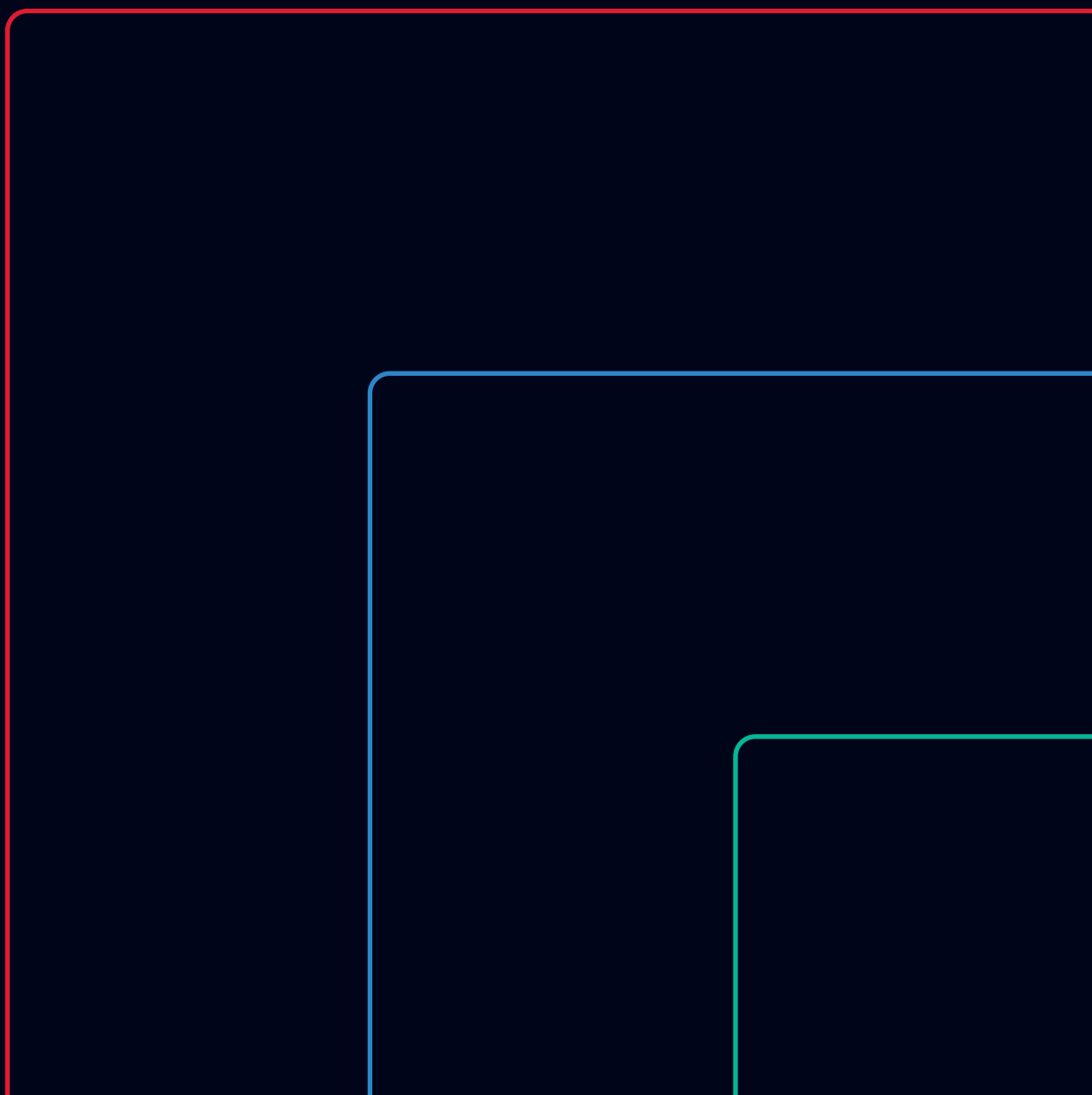# Cyber Security Policy

# Cyber Security Policy

This policy ensures the security and integrity of Unitary Engineering Service's data and IT infrastructure. This policy applies to all employees, contractors, and business partners who access our network and data.

## Data Protection & Compliance

All personal customer data, financial information, and sensitive business information must be handled in compliance with GDPR and other relevant data protection laws. Regular training on data protection principles will be provided to all staff.

## Access Control

Access to sensitive information is restricted based on role-specific needs. For instance, only the Accounts department can access detailed financial records. The outsourced IT company (Rakata Technology Ltd) will manage access levels and ensure they are updated as per role changes within the company, discussing requirements with the Managing Director, Adam Griffiths.

## Physical and Network Security

Physical access to our facilities and digital access to our networks are secured and monitored. Firewalls, anti virus software, and other security measures will be maintained and updated regularly.

## Data Encryption and Backup

Sensitive data will be encrypted both in transit and at rest. Regular backups of all critical data will be conducted and stored securely.

## Incident Response and Reporting

In the event of a security breach or suspicion thereof, immediate reporting to the designated security officer is mandatory. A response plan will be in place to address any security incidents swiftly and effectively.

## Remote Access and Mobile Device Management

While remote work is not a common practice, any exceptions must adhere to strict security protocols, including secure VPN access and end-to-end encryption.

Company-issued mobile devices will be equipped with necessary security features and regularly monitored.

Regular Audits and Assessments

Regular security audits will be conducted to assess the effectiveness of existing security measures. Vulnerability assessments will be performed periodically to identify and mitigate potential risks.

Third-Party Vendors and Partners

All third-party vendors, including our outsourced IT company, must comply with our security policies and GDPR requirements. Regular reviews of third-party security policies and practices will be undertaken.

Policy Review and Update

This policy will be reviewed annually or in response to significant changes in our IT infrastructure or data handling practices. All employees will be notified of any changes to the policy.

Date:       04.08.2023

Name:       Adam Griffiths

Signed:

Managing Director

Unitary Engineering Services Ltd