Cyber Security Policy

1. Introduction

This policy outlines the measures and procedures to ensure the security of our digital assets and compliance with UK cyber security laws and regulations.

2. Scope

This policy applies to all employees, contractors, volunteers, and anyone with permanent or temporary access to our systems and hardware.

3. Legal and Regulatory Compliance

We comply with the following UK laws and regulations:

- Data Protection Act 2018 (DPA 2018): Ensures the protection of personal data.
- UK General Data Protection Regulation (UK-GDPR): Regulates data protection and privacy.
- Data (Use and Access) Act 2025 (DUAA) – including recognised legitimate interests, automated decision-making safeguards, updated cookie/tracking rules, and the mandatory data-protection complaints process effective 19 June 2026.
- Network and Information Systems (NIS) Regulations: Enhances the security of network and information systems.
- Computer Misuse Act 1990: Addresses unauthorized access to computer systems.
- Telecommunications (Security) Act 2021: Ensures the security of telecommunications networks.
- Updated Telecommunications Security Code of Practice compliance (2025 revision).
- Note: NIS reforms under the Cyber Security and Resilience Bill expanding reporting duties and supply-chain oversight.

4. Risk Management

Regular risk assessments, vulnerability testing, security controls, and maintenance of an incident response plan.

5. Access Control

Access to information systems is restricted based on the principle of least privilege. Measures include:

- Least Privilege
- Strong password policies.
- Multi-factor authentication.
- Regular review of access rights.

6. Data Protection

We ensure the confidentiality, integrity, and availability of data by:

- Encrypting sensitive data.
- Regularly backing up data.
- Implementing data loss prevention measures.
- Secure Transfer
- DUAA Aligned Processing Rules

7. Incident Response

In the event of a cyber incident, we will:

- Follow the incident response plan.
- Report incidents to relevant authorities as required by law (including NIS expectations)
- Conduct post-incident reviews to improve our security posture.

8. Training and Awareness

Mandatory annual training including DUAA and updated regulatory responsibilities.

9. Monitoring and Review

We continuously monitor our information systems for security threats and regularly review this policy to ensure it remains effective and compliant with current laws and regulations.

10. Responsibilities

All employees are responsible for adhering to this policy.

11. Confidential Data

Confidential data is secret and valuable. Common examples include:

- Unpublished financial information.
- Data of customers, partners, and vendors.
- Patents, formulas, or new technologies.
- Customer lists (existing and prospective).
- IP
- Employee information

All employees are obliged to protect this data. This policy provides instructions on how to avoid security breaches.

12. Device Protection

When employees use their digital devices to access Rayan Facilities Management Ltd emails or accounts, they introduce security risks to our data. We advise our employees to keep both their

personal and Rayan Facilities Management Ltd-issued computers, tablets, and cell phones secure. They can do this by:

- Keeping all devices password protected.
- Choosing and upgrading comprehensive antivirus software.
- Ensuring they do not leave their devices exposed or unattended**.**
- Installing security updates for browsers and systems monthly or as soon as updates are available.
- Logging into Rayan Facilities Management Ltd accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others. When new hires receive Rayan Facilities Management Ltd-issued equipment, they will receive instructions for:

- Password management tool setup.
- Installation of antivirus/anti-malware software.

They should follow these instructions to protect their devices and refer to our Security Specialists/Network Engineers if they have any questions.

13. Email Safety

Emails often host scams and malicious software (e.g., worms). To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing").
- Be suspicious of clickbait titles (e.g., offering prizes, advice).
- Check the email addresses and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks).

If an employee isn't sure that an email they received is safe, they can refer to our IT Specialist.

14. Password Management

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g., birthdays).

- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

Remembering a large number of passwords can be daunting. We will advise on a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the aforementioned advice.

15. Data Transfer

Transferring data introduces security risks. Employees must:

- Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless absolutely necessary.
- Encrypted Transfers
- Share confidential data over the Rayan Facilities Management Ltd network/system and not over public Wi-Fi or private connections.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.

16. Reporting Security Incidents

We advise our employees to report perceived attacks, suspicious emails, or phishing attempts as soon as possible. We must investigate promptly, resolve the issue, and send a Rayan Facilities Management Ltd-wide alert when necessary. We are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

17. Additional Measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HR/IT Department.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in Rayan Facilities Management Ltd systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on their Rayan Facilities Management Ltd equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy.

18. Remote Employees

Remote employees must follow this policy's instructions too. Since they will be accessing Rayan Facilities Management Ltd's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, patching and ensure their private network is secure. DUAA Compliant Data Handling.

19. Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated, or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.

We will examine each incident on a case-by-case basis. Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

20. Data Protection Complaints Handling (DUAA Requirement)

Rayan FM will operate a formal internal complaints procedure for data protection concerns from 19 June 2026.

21. General Security Awareness

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Signed:

Name: Siobhan Hamill

Position: Managing Director

Date: 01/02/2026