Helios Fire & Construction Consultancy Ltd - IT & Website Systems Policy

DATE:	14th November 2025	CONFIDENTIALITY:	Confidential
SUBJECT:	IT & Website Systems Policy	AUTHOR/ REVIEWER:	DJD / RJ
PROJECT NUMBER:	Version 01	REVISION:	01

1. Purpose

This policy defines the standards, responsibilities and acceptable practices for the management, use and protection of the IT systems, networks, and website operated by Helios Fire & Construction Consultancy Ltd ("the Company").

Its goal is to safeguard information assets, maintain the confidentiality, integrity and availability of systems, and ensure compliance with relevant UK laws, including the Data Protection Act 2018 and the UK GDPR.

2. Scope

This policy applies to:

- All employees, contractors, consultants, temporary staff and third parties who use or access the Company's IT systems.
- All devices, software, networks, communications, cloud services and the public-facing company website.
- All information processed, transmitted, or stored on these systems.

3. Roles and Responsibilities

Management

- Approves and enforces this policy.
- Provides resources to maintain IT security and compliance.

IT Administrator / Service Provider

- Implements technical and security controls.
- Manages backups, patching, updates, access control and incident response.

Employees and Users

- Use systems responsibly and only for legitimate business purposes.
- Protect company data and follow this policy at all times.
- Report any suspected security incident or data breach immediately to management.

4. Web Based Document Management Systems

Should a web-based document management system be used by our clients, information that is specifically required to be assessed and reviewed by Helios Fire & Construction Consultancy should be issued directly to the representative of Helios Fire & Construction Consultancy. The acceptance of access onto any web-based system by Helios Fire & Construction Consultancy does not constitute an acknowledgement that all information on the specific portal will have been assessed and reviewed.

5. Access Control

- Access to systems and data is granted on a need-to-know basis.
- Every user must have a unique account and password.
- Passwords must be at least 6 characters long and include letters, numbers and symbols.
- Multi-Factor Authentication (MFA) must be enabled where possible
- Access rights are reviewed regularly and revoked when no longer required.

6. Data Protection & Privacy

- Our Data Protection & Privacy policy is covered under the ICO Privacy Notice/GDPR policy document which can be downloaded separately from the Policy section of our website.

Helios Fire & Construction Consultancy Ltd

© 2025 Helios Fire & Construction Consultancy Ltd – All rights reserved.

7. Email and Communication

- Business email accounts are the property of the Company and may be monitored for security and compliance.
- Emails must not contain discriminatory, defamatory, or confidential information sent to unauthorised recipients.
- Phishing or suspicious messages must be reported immediately.
- Sensitive attachments should be encrypted or password protected.

8. Backups and Business Continuity

- Regular backups of important data and systems must be performed (at least daily for critical data).
- Backup copies must be stored securely and tested regularly.
- A disaster recovery plan must be maintained to restore operations in case of system failure or data loss.

9. Security and Incident Management

- All devices must have active antivirus/antimalware protection and firewalls enabled.
- Suspicious activity or security breaches (e.g., data loss, unauthorised access, malware infection) must be reported immediately to management.
- The Company will investigate incidents promptly, contain threats, and take corrective actions.
- Personal data breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours if required by law.

10. Monitoring and Logging

- IT systems, networks and internet usage may be logged and monitored for security, compliance and performance reasons.
- Monitoring will be conducted lawfully and proportionately under the Investigatory Powers Act 2016 and data protection law.

11. Review and Maintenance

- This policy will be reviewed annually, or sooner if there are significant changes in technology, business operations or legal requirements.
- Updates will be communicated to all staff and stakeholders.