

Cyber Security Policy

Purpose

The purpose of this Cyber Security Policy is to set out Capital Sky's commitment to cyber security and confirm the functional responsibilities of management, devolved divisions, and all colleagues towards achieving these objectives.

This policy forms part of Capital Sky Ltd's Integrated Management System (IMS) and supports compliance with ISO 27001:2022 principles for information security management, alongside ISO 9001:2015, ISO 14001:2015, and ISO 45001:2018 where information systems support operational delivery. The policy aligns with the UK Government Cyber Essentials scheme as part of the organisation's baseline technical cyber security controls. It also supports compliance with applicable legislation including the [Data Protection Act 2018](#) and [UK GDPR](#), the [Computer Misuse Act 1990](#), and where applicable the [Network and Information Systems Regulations 2018](#). In the context of construction operations, it also supports secure management of digital safety-critical information in line with the [Building Safety Act 2022](#) and associated "Golden Thread" principles, including dutyholder information management requirements under the [Building Regulations 2010 \(as amended\)](#).

Objective

The objective of cyber security is to minimise the risk of harm to, or destruction of, computer networks, applications, devices, and data.

This includes protection of business systems, personal and commercial data, intellectual property, and construction-related safety-critical information. Failure to adequately secure these assets may result in operational disruption, loss of data, regulatory penalties including ICO enforcement, reputational damage, financial loss, and legal consequences.

Responsibilities

This policy applies to all employees, suppliers, contractors, consultants, agency workers, and any other persons granted access to Capital Sky information systems or digital assets.

All users are required to use systems, data, and technology in accordance with this policy, the Code of Ethics and Conduct, and applicable legal and contractual requirements. Non-compliance may result in disciplinary action, termination of contract, withdrawal of system access, and in serious cases criminal or civil proceedings.

Policy Principles

Capital Sky manages cyber security risk through a risk-based approach aligned with ISO 27001 principles and integrated business risk management processes. Cyber risks are identified, assessed, and escalated where they may impact operational performance, client delivery, or legal compliance. Business areas are responsible for ensuring that appropriate security controls are implemented within their systems and processes. The Cyber Security function provides governance, oversight, and technical guidance across the organisation, ensuring consistency of controls and continuous improvement.

Security controls are applied proportionately to risk and include protection of sensitive business data, personal data, and construction project information, including Building Safety Act "Golden Thread"

information where applicable. Such information must remain accurate, traceable, version controlled, and protected against unauthorised alteration throughout its lifecycle, in line with regulatory expectations for information management and safety case evidence.

Information Security Requirements

Capital Sky maintains minimum security requirements to protect information assets. Access to systems is restricted based on role and business need, applying the principle of least privilege. Access rights are reviewed periodically and are removed or amended promptly when roles change or employment ends. Strong passwords are required and must not be shared between users. Multi-factor authentication is implemented where systems allow.

Employees and users must use Capital Sky systems responsibly and only for authorised business purposes. This includes appropriate use of email, internet access, and digital platforms. The use of unauthorised software, unapproved cloud services, or external file-sharing systems is not permitted unless explicitly authorised.

Use of cloud services and third-party software must be formally approved to ensure security, data protection compliance, and appropriate contractual controls are in place.

Removable media (including USB devices and external storage) must only be used where necessary and must be approved and appropriately secured to prevent loss, theft, or malware infection.

Where personal or mobile devices are authorised, they must be encrypted, password protected, and capable of remote wipe. Loss or suspected compromise must be reported immediately.

Company data must only be stored and processed on approved systems and devices. All processing of personal data is carried out in accordance with [UK GDPR](#) principles of lawfulness, fairness, transparency, data minimisation, accuracy, storage limitation, integrity, and confidentiality.

Information relating to construction projects, including safety-critical and regulatory documentation, must be protected against loss, unauthorised access, alteration, or destruction. This includes digital systems supporting [Building Safety Act 2022](#) obligations and project delivery information.

All systems are subject to appropriate logging and monitoring to support detection, investigation, and response to security incidents.

Data backups are maintained to support business continuity and disaster recovery requirements and are subject to periodic restoration testing to confirm recovery capability.

Capital Sky applies a data classification approach to ensure appropriate handling of information. Data is classified as Confidential, Internal Use, or Public.

All employees are required to handle information in accordance with its classification level, ensuring that confidential and commercially sensitive data is protected from unauthorised access, disclosure, alteration, or loss.

Phishing and social engineering risks must be treated seriously. Users must not click suspicious links or open unexpected attachments and must report any suspected phishing attempts immediately.

Functional Responsibilities

Management Responsibilities

Management are responsible for ensuring that cyber security is actively supported across the organisation through appropriate governance, resourcing, and oversight. They act as escalation points for significant cyber incidents and ensure that third parties and internal teams are aware of their responsibilities under this policy.

Management must ensure that cyber security requirements are embedded within operational processes, procurement arrangements, and contractual obligations, and that compliance is maintained with ISO standards and relevant legislation.

Directors and Managers

Directors and managers are responsible for owning cyber security risks within their areas of control and ensuring that these are appropriately assessed and managed. They must promote cyber security awareness, ensure staff complete mandatory training (at induction and at least annually), and support the implementation of effective controls.

They are also responsible for ensuring that business continuity and disaster recovery arrangements are in place and remain suitable for operational needs. Where applicable, they must ensure that digital project information, including Building Safety Act “Golden Thread” data, is adequately protected and controlled throughout its lifecycle.

All Employees and Users

All individuals are responsible for completing cyber security awareness training and for complying with this policy at all times. They must take reasonable care when handling data, protect access credentials, and ensure that information is not disclosed, transferred, or stored in an insecure or unauthorised manner.

Any suspected cyber security incident, weakness, or breach must be reported immediately through the appropriate reporting channels.

Cyber Security Function

The Cyber Security function is responsible for maintaining and developing the organisation’s cyber security framework in line with ISO 27001 principles. This includes establishing policies and standards, supporting risk management, advising on technical controls, and coordinating incident response activities.

It is also responsible for promoting awareness across the organisation, maintaining industry engagement, and ensuring continuous improvement of cyber resilience capability in line with evolving threats and regulatory expectations.

Incident Management and Reporting

All suspected or actual cyber security incidents must be reported without delay. This includes data breaches, unauthorised access, malware infection, phishing attacks, loss or theft of devices, or compromise of business or project systems.

Incidents are managed through a structured process of identification, containment, investigation, recovery, and post-incident review.

Where personal data is involved, Capital Sky will comply with UK GDPR requirements, including reporting to the Information Commissioner's Office (ICO) within statutory timeframes where applicable.

Where a cyber security incident is identified, immediate containment actions will be taken where possible, followed by escalation to the Cyber Security function and relevant management. Where required, incidents involving personal data will be assessed for notification to the Information Commissioner's Office (ICO) in accordance with UK GDPR breach reporting requirements.

Supplier and Third-Party Security

All suppliers and subcontractors with access to Capital Sky systems, data, or project information must comply with this policy or demonstrate equivalent cyber security controls. Suppliers are assessed on a risk-based approach, taking into account the type of data accessed, system connectivity, and operational criticality. Higher-risk suppliers may be subject to additional assurance measures including security questionnaires, contractual controls, and periodic review. All third parties are required to protect confidential, personal, and project-related information and ensure that appropriate safeguards are in place to prevent unauthorised access, loss, or cyber compromise. Security obligations must be flowed down to subcontractors where applicable.

Continuous Improvement

Capital Sky is committed to continual improvement of its cyber security arrangements through monitoring, internal review, audit activity, risk assessment, and lessons learned from incidents. The policy will be updated to reflect changes in legislation, ISO standards, NCSC guidance, and industry best practice.

This policy will be reviewed at least annually, or following significant changes to legislation, organisational structure, systems, or cyber risk profile.

Name: Martin Maloney

Position: Chief Executive Officer

Signature:



Dated: 15/05/2026

Latest Review Date: 15/05/2027