

Information Security Policy

1. Purpose

The purpose of this policy is to define Chase Services Group's approach to managing information security in compliance with ISO/IEC 27001:2022 and other regulatory requirements, ensuring the confidentiality, integrity, and availability of all business information.

2. Scope

This policy applies to all operations, employees, contractors, third parties, and IT systems handling information owned or managed by Chase Services Group.

3. Information Security Objectives

Protect organisational and client information from unauthorised access, alteration, disclosure, or destruction. Ensure the reliability and continuity of information systems. Comply with UK GDPR, Data Protection Act 2018, contractual obligations, and client requirements. Maintain and improve our ISO/IEC 27001:2022 Information Security Management System (ISMS).

4. Governance and Responsibilities Board of Directors

Provide leadership and ensure adequate resources. Information Security Manager/DPO: Maintain the ISMS, oversee risk assessments, and monitor compliance. All Staff: Responsible for adhering to this policy and reporting incidents promptly.

5. Risk Management

Information security risks are identified, evaluated, and treated using a risk-based approach. Risk assessments are reviewed annually or after major changes to systems or processes.

6. Access Control

Access to systems and data is based on the principle of least privilege. Authentication mechanisms (e.g., passwords, MFA) are enforced, and access rights are reviewed regularly.

7. Data Protection and Privacy

Chase Services Group is registered with the Information Commissioner's Office (Reg. No: [insert number]) and complies with the Data Protection Act 2018 and UK GDPR. We maintain a detailed Data Protection Policy that governs data processing, retention, and deletion practices.

8. Asset Management

All assets are inventoried and classified according to sensitivity and criticality. Data storage devices are securely wiped or destroyed before disposal.

9. Physical and Environmental Security

Access to offices and data storage areas is restricted to authorised personnel only. Physical security controls include CCTV, access cards, and secure disposal of confidential materials.

10. Incident Management

All security incidents are logged, investigated, and resolved following our Incident Response Procedure. Major incidents are escalated to the DPO and management immediately.

11. Business Continuity and Disaster Recovery

Continuity plans ensure critical business operations can continue in the event of system failures or disasters. Data backups are performed regularly and tested periodically.

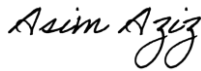
12. Training and Awareness

All staff receive regular training on information security, GDPR compliance, and phishing awareness.

13. Review and Continuous Improvement

This policy is reviewed annually as part of the ISMS continual improvement process. Updates are communicated to all employees.

Signed



Date

01/09/2026

Managing Director