TUTELA GROUP

BUILD • MAINTAIN • SPECIAL PROJECTS

TUTELA GROUP

POLICY DOCUMENT

ISO 27001
INFORMATION
SECURITY POLICY

ISO 27001 Information Security Policy

1. Purpose and Scope

The Tutela Group is committed to protecting its information assets and ensuring the confidentiality, integrity, and availability of data in all our operations, including construction, fit out, refurbishment, facilities maintenance, and special projects services. This Information Security Policy establishes a comprehensive framework for managing and safeguarding information, in alignment with the ISO 27001 standard. It applies to all employees, contractors, and third parties who have access to our information systems and data.

2. Policy Statement

"The Tutela Group is dedicated to implementing and maintaining an effective Information Security Management System (ISMS) that complies with ISO 27001 requirements. We commit to continuously managing information security risks and ensuring that our processes, technologies, and practices protect our information assets from threats, thereby upholding the trust of our clients, employees, and stakeholders."

3. Information Security Objectives

Confidentiality: Protect sensitive information from unauthorized access.

Integrity: Ensure the accuracy and reliability of data through robust controls.

Availability: Guarantee that information and services are accessible to authorized users when needed.

Risk Management: Identify, assess, and mitigate information security risks in a proactive and systematic manner.

Compliance: Adhere to all applicable legal, regulatory, and contractual requirements related to information security.

4. Key Principles and Controls

Access Control:

Implement role-based access controls and enforce strict user authentication measures to ensure that only authorized personnel have access to critical information.

Regularly review and update access privileges based on job roles and responsibilities.

Physical Security:

Secure physical access to IT facilities and sensitive areas to prevent unauthorized entry.

Employ surveillance, secure entry systems, and visitor management procedures.

Technical Security:

Utilize industry-standard security measures including firewalls, encryption, antivirus software, and intrusion detection systems.

Regularly update and patch software to protect against known vulnerabilities.

Incident Management:

Establish an incident response plan to detect, respond to, and recover from security incidents promptly.

Ensure that incidents are reported, documented, and reviewed to improve future responses.

Data Management:

Enforce data classification, handling, and disposal procedures to maintain data integrity and confidentiality.

Ensure that backups and disaster recovery measures are in place to secure critical data.

Training and Awareness:

Provide regular information security training to employees and contractors to raise awareness and promote best practices.

Encourage a culture of security mindfulness and continuous improvement.

Risk Assessment:

Conduct regular risk assessments and audits to identify vulnerabilities and assess the effectiveness of existing controls.

Implement corrective measures to address identified risks in a timely manner.

5. Roles and Responsibilities

Senior Management:

- Provide strategic direction and ensure the allocation of necessary resources to support the ISMS.
- Champion information security as a core business priority.
- Information Security Manager / Data Protection Officer:
- Oversee the implementation, management, and continuous improvement of the ISMS.
- Coordinate risk assessments, incident management, and compliance audits.

IT Department:

- Implement and maintain technical security controls and monitor systems for potential threats.
- Ensure system configurations align with the organization's security policies and standards.

All Employees and Contractors:

- Adhere to this policy and all related procedures.
- Report any security incidents or suspicious activities to the designated Information Security Manager immediately.

6. Policy Compliance and Enforcement

Monitoring and Review:

Regularly monitor compliance with this policy through internal audits and risk assessments.

Review and update the policy periodically to address emerging threats and changes in legal or business requirements.

Non-Compliance:

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships.

Any detected breach will be investigated promptly, and corrective actions will be implemented.

Continuous Improvement:

The Tutela Group is committed to continuous improvement of its ISMS through regular feedback, audits, and updates to security practices.

7. Communication and Training

The contents of this policy will be communicated to all employees, contractors, and relevant third parties.

Regular training and awareness programs will be conducted to ensure understanding of security responsibilities and the importance of safeguarding information.

By implementing this ISO 27001 Information Security Policy, The Tutela Group reaffirms its commitment to protecting its information assets, maintaining the highest security standards, and fostering a secure environment for all stakeholders involved in our operations.

Issue Date: 17/11/25

Issued By: Robert Taylor

Position: Managing Director

Review Date: 17/11/26

TUTELA GROUP

www.tutela-group.co.uk