INSERT LOGO

INFORMATION SECURITY POLICY

Classification: **Public**

This document may be shared with interested parties outside of [Company Name]

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Contents

Purpose of This Document

This policy outlines [Company Name] 's overarching approach to information security management and signposts to specific sub-policies within the framework.

Scope

Applicability

The Information Security Policy applies to

- All organisational and customer information, regardless of format.
- All individuals associated with [Company Name], including temporary workers and external contractors.

Context of Information Security

The scope and context of information security, including the internal and external factors affecting [Company Name], is documented in the 'Information Security Management System (ISMS) Scope Document', which can be accessed here: [provide location or method of access]."

Roles & Responsibilities

Information Security Group (ISG):

- Approve and oversee the security policy.
- Manage the Information Security Management System (ISMS) framework.
- Guide and support security efforts within [Company Name].

Information Security Manager:

- Manage the ISMS.
- Handle security risk assessments

- Ensure adherence to the ISMS

System / Information Owners:

- Manage security risks within their remit.
- Support the Information Security Manager.
- Ensure compliance with data procedures and policies.

Line Managers:

- Grant access based on role needs
- Ensure policy compliance within their teams
- Manage access and return of [Company Name] devices and systems

All Staff:

- Comply with the policy and related procedures.
- Report policy breaches.
- Seek exceptions via the IT Helpdesk.

For more information on roles & responsibilities, please see the ISMS Roles and Responsibilities Document.

Related ISMS Policies

To ensure comprehensive information security management, [Organisation Name] has established several detailed policies that support and complement this Information Security Policy.

Employees, contractors, and other stakeholders are required to familiarise themselves with these policies and adhere to their guidelines.

The related policies include:

Policy Name	Description
Acceptable Use Policy	Defines acceptable and unacceptable use of the organisation's information systems and resources.
Access Control Policy	Specifies the requirements for controlling access to information and information systems.
BYOD Policy	Establishes rules and guidelines for using personal devices to access company data and systems.
Data Protection Policy	Details measures and practices to protect personal data in compliance with relevant regulations.
Data Retention Policy	Sets out the principles for retaining and disposing of data in a secure and compliant manner.
Mobile Device Policy	Provides guidelines for the secure use of mobile devices within the organisation.

Password Policy	Defines the requirements for creating, managing, and protecting passwords.
Patching Policy	Describes the process for managing software patches and updates to maintain security.
Secure Development Policy	Outlines best practices for developing and maintaining secure software applications.
Supplier Security Policy	Establishes security requirements for engaging and managing third-party suppliers.
Asset Management Policy	Details procedures for managing information assets throughout their lifecycle.
Cloud Services Policy	Provides guidelines for the secure use and management of cloud services.
Remote Working Policy	Specifies security measures and practices for employees working remotely.

Information Security Objectives

- The ISG working group sets annual objectives, which are reviewed quarterly.
- Objectives are stored in the following location: [location of information security objectives].

Training and Awareness

- All staff and contractors must undergo security training to support their roles. The training must align with their job roles and the data they handle.
- Induction for new employees includes mandatory security awareness.
- Staff will be given regular training updates to maintain awareness of changing security threats.

Physical Security

- Staff will secure and report lost security access passes.
- Use physical restrictions such as key or swipe cards to manage access to restricted areas and equipment.
- Always ensure visitors are accompanied on site.

Oral Communications

- Use caution when communicating confidential information in public areas due to the risks of being overheard.

Third-Party Security

- All third parties processing data on behalf of the organisation will undergo a risk assessment.
- All third parties handling internal or confidential information must sign confidentiality agreements.

- The organisation's security policies will be communicated to third parties and contractually obligated as required.
- Refer to related third-party security policies;
    i. Software as a Service (Saas) Policy: To introduce any new cloud-based applications.
    ii. Supplier Security Policy: This is for guidance on expectations around the approach to 3rd party security, with particular emphasis on personal data protection.

Employment Screening

- The organisation will undertake background checks as part of the employment process.

Restricting Unauthorised Access

- Seek explicit, written authorisation for sharing sensitive data.
- Access rights will be managed in alignment with the Access Control Policy
- The principle of least privilege is used to grant individuals minimal access to data.
- Regularly audit information to ensure only authorised individuals have access.

Appropriate Use of Security Credentials

- For further details, please refer to the Password Policy.
- Staff and contracted parties must safeguard and not share personal security credentials.
- Enable Multi-Factor Authentication where possible.

Cryptographic Controls

- Procedures for generating, distributing, rotating, and destroying cryptographic keys will be maintained.
- Keys will be stored in a central, restricted storage location.
- Regularly review and update the list of approved algorithms to adapt to technological advancements and emerging threats.

Information Classifications

Classifications communicate the confidentiality level of information and with whom it can be shared. To this end, [Company Name] has defined three levels of classification outlined below.

"Confidential" Information

- Unauthorised disclosure of this information to people without a business need for access may violate laws and regulations or cause significant problems for [Company Name], its customers, or its business partners.
- The information owner or an appropriate manager must approve access to confidential information.
- Examples of Confidential Information may include:
    - personal information

  - customer information
  - company financial information
  - information on commercial relationships
  - system access IDs and passwords
  - file encryption keys.

Handling Guidance for Confidential Information

- **Encryption:** Ensure all confidential data, both in transit and at rest, is encrypted using approved encryption methods.
- **Access Control**: Limit access strictly to authorised personnel with a legitimate need for access.
- **Data Storage**: Store in secure, access-controlled environments (physical or digital).
- **Data Transfer**: Use secure, encrypted channels for transferring confidential data.
- **Destruction and Disposal**: Confidential data should be securely and irreversibly destroyed when no longer needed. This includes paper documents, digital files, and any removable media.
- **Breach Protocol:** Establish a specific protocol for reporting and responding to confidential information breaches.

"Internal" Information

- Information intended for unrestricted use within [Company Name] and, in some cases, within affiliated organisations such as [Company Name] business partners.
- It may be distributed within [Company Name] without advance permission from the information owner.
- Any information not explicitly classified as Confidential or Public will, by default, be classified as Internal Information.
- Unauthorised disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.
- Examples of Internal Information may include:
  - personnel directories
  - internal policies and procedures
  - most internal electronic mail messages.

Handling Guidance for Internal Information

- **Encryption:** Internal information will be encrypted in transit and at rest.
- **Access Control**: Access should be limited to the organisation's staff and contracted parties but not shared externally without written permission.
- **Data Storage**: Data will be stored in secure, access-controlled environments.
- **Data Transfer**: Care should be taken, but encrypted transfer is unnecessary.
- **Destruction and Disposal**: Internal data should be securely and irreversibly destroyed when no longer needed. This includes paper documents, digital files, and any removable media.

- **Breach Protocol:** Establish a specific protocol for reporting and responding to confidential information breaches.

"Public" Information

- Public information has been approved for public release by a designated authority within [Company Name].
- This information may be disclosed outside of [Company Name].
- Examples of Public Information may include:
    - marketing brochures
    - material posted to [Company Name] websites
    - [Company Name] posts to social media sites.

Handling Guidance for Public Information

- **Encryption:** Public information is not encrypted.
- **Access Control**: Access to duplicates of public information is not restricted, and information can be freely shared. The source information will be strictly controlled as 'internal information', for example, company information brochures, website information, etc.
- **Data Storage**: Data may be stored on a variety of platforms.
- **Data Transfer**: Care should be taken, but encrypted transfer is unnecessary.
- **Destruction and Disposal**: Public information does not require planning and control for destruction but may require consideration for information retirement to ensure obsolete data is not propagated.
- **Breach Protocol:** None.

Breaches of Security

- Report system security concerns immediately to the IT Helpdesk.
- Report physical breaches to the Office Manager or CPO.
- Please Refer to the Data Protection Policy for personal data breaches.
- Please refer to the Information Security Incident process for significant data breaches.

Associated Policies and Documents

The following policies support and provide additional context to this policy and responsibilities.

Policy	Description	Location
Acceptable Use Policy	Guides staff on how the organisation's technology may be used.	
Data Protection Policy	How personally identifiable data will be handled.	

Password Policy	Outlines the password complexity and usage.	
Mobile Phone Policy	Details usage of company-provided mobile phones.	
SaaS Policy	Summarises how cloud-based software solutions can be evaluated and introduced into the organisation.	
Bring-Your-Own-Device Policy	Outlines how personal devices can be used for organisational purposes.	
Access Control Policy	How access and security rights to systems are granted and controlled.	
Supplier Security Policy	Summarises how 3rd parties processing the organisation's data must be managed.	

Monitoring and Filtering

- [Company Name] monitors its IT systems to ensure they align with applicable legislation.
- Logging and investigations ensure security and policy adherence.

Risk Assessment & Treatment Methodology

As an integral part of our Information Security Management System (ISMS), [Company Name] is committed to identifying, assessing, and managing information security risks. We adhere to a structured Risk Assessment and Treatment Methodology outlined in a separate document to achieve this.

The Risk Assessment and Treatment Methodology includes:

- **Risk Identification:** Systematically identifying potential security threats and vulnerabilities that could impact our information assets and business operations.
- **Risk Analysis and Evaluation:** Assessing the likelihood and potential impact of identified risks, enabling prioritisation based on our risk appetite and business objectives.
- **Risk Treatment:** Determining the most appropriate risk treatment options, which may include risk avoidance, risk reduction, risk sharing, or risk acceptance.
- **Monitoring and Review:** Regularly monitor and review risks and the effectiveness of the implemented treatment measures to ensure continuous improvement of our ISMS.
- **Communication and Consultation:** Ensuring effective internal and external communication and consultation throughout the risk management process.

This methodology aligns with the principles and guidelines of ISO 27001 and supports our commitment to maintaining a robust information security posture.

For detailed procedures and guidelines on conducting risk assessments and selecting appropriate risk treatment options, please refer to the [Risk Assessment and Treatment Methodology Document]. This document is accessible [specify the location or how to access the document, e.g., on the organisation's internal portal, document management system, etc.] and is maintained by the Information Security Group (ISG).

All staff and relevant external parties are responsible for familiarising themselves with the methodology outlined in the document and contributing to the ongoing identification and management of information security risks within their work areas.