INSERT LOGO

INFORMATION SECURITY MANAGEMENT SYSTEM SCOPE

Commented [AP1]: Before using this document, set the company name.

Search and replace "[company name]" for your organisation's name.

Classification: **Internal**

This document may only be shared internally without prior confirmation from the owner.

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

Contents

Information Security Management System Scope

Purpose of Document

This document outlines the scope of [Company Name]'s Information Security Management System (ISMS), including the parts of our organisation, processes, and systems that are covered by the ISMS.

The guidance ensures everyone, from employees to management, understands the extent of our information security efforts. It also aligns our ISMS with our business goals, legal requirements, and contractual obligations.

Commented [AP2]: Why do we have this document?

It lays out the Info Sec stall to all interested parties, including auditors. It says, 'This is our organisation, this is the scope of the services, processes, and technologies, and these are the factors we consider in any decisions we make regarding security.

Introduction

[Provide a brief overview of your organisation, explaining its purpose and services. This provides a useful overview for anyone not familiar with the organisation, such as auditors and external 3rd parties.]

Scope Statement

[Provide a concise summary of what is included in the ISMS scope, summarising the details below. The following is an example.]

Commented [AP3]: Tip: If this is your first attempt at 27001, then keep the scope tight, maybe around any systems or services processing client or employee information. This ensures you don't overdo it, and make things too complicated. Start as small as possible, and build out the scope in future years.

The scope of the Information Security Management System (ISMS) at [Company Name] encompasses the protection of all information assets related to our core business operations, including customer data, intellectual property, and internal communications.

Purpose of the ISMS

At [Company Name], our ISMS aims to protect our information assets and ensure data confidentiality, integrity, and availability. The ISMS supports maintaining customer trust, meeting legal obligations, and safeguarding intellectual property.

Information Security Management System Scope

We focus on managing information security risks by identifying, assessing, and mitigating them according to our risk appetite and business strategy.

Our ISMS complies with regulatory, legal and contractual requirements, showing our commitment to regulatory compliance and operational excellence.

Implementing the ISMS demonstrates our dedication to top-tier information security practices.

We are committed to continuous improvement, regularly updating our security measures to adapt to new threats and business changes.

Context of the Organisation

Internal Issues

Organisational Structure

[Outline the company's hierarchy, departments, and functions. Include a high-level organisational chart.]

Business Processes

[Clarify the organisation's business process at a high-level so the reader gains context of what the organisation does. This should include all major processes (e.g., finance, customer support, development). Include a high-level diagram showing how information flows and is protected.]

Interested Internal Stakeholders

The following are the key internal stakeholders who have an active interest in Information Security within [Company Name].

Stakeholder	Requirements
Senior Management	Aligning ISMS with business goals, ensuring legal compliance, managing risks, and protecting reputation.
IT Department	Implementing technical security measures, managing IT infrastructure, and responding to incidents.
Human Resources	Employee training on information security, managing personnel security, and handling confidential employee data.
Legal and Compliance Team	Ensuring compliance with laws and contracts, advising on security breaches, and managing data protection.
Finance Department	Budgeting for ISMS, analysing security investments, and understanding the financial impacts of incidents.
Operations/Production Teams	Ensuring operational continuity, protecting operational data, and minimising disruptions from incidents.

Sales and Marketing	Protecting customer data, ensuring compliance, and using secure communication channels.
Research and Development	Securing intellectual property, integrating security in development, and managing access to research data.
Customer Service/Support	Safeguarding customer information, handling data security queries, and responding to incidents.
Staff	Require confidence of management of personal data.

External Issues

Legal, Regulatory, and Contractual Obligations

[List any major internal information security requirements, such as employment contracts, internal policies, or customer contracts. Note, this differs from the external legal obligations explored in the next section, such as GDPR, etc]

Description	Requirement
Contract – ING Limited	Our contract with ING stipulates ISO 27001 as a requisite, and must be demonstrated every year.
GDPR	EU regulation for data protection, applicable to businesses handling EU/UK citizens' data.
Data Protection Act 2018 (DPA 2018):	UK's implementation of GDPR, requiring data protection.

Commented [AP4]: All the following are examples to get your going, and will depend on where you are undertaking business and the nature of it.

Technical Environment

[Note any technology advancements or emerging cyber risks impacting security, such as the increased landscape for ransomware in similar organisations. Current threats for types of organisations (e.g. charities, etc) can be found online.]

Market & Industry Conditions

[Summarise trends in your industry affecting information security, such as emerging threats or new technologies.]

External Stakeholders

The following outlines the key stakeholders outside of [Company Name] who may have an interest in the ISMS.

External Stakeholder	Requirements
Customers/Clients	Assurance of data protection, service reliability, transparency in data handling.

Suppliers and Vendors	Security in the supply chain, protection of shared information, compliance with security policies.
Regulatory Authorities	Compliance with security standards, incident reporting, adherence to data protection laws.
Partners and Investors	Confidence in risk management, security's role in business stability, protection of shared intellectual property.
Certification Bodies	Compliance with certification standards, adequacy of security controls, regular audits for continuous improvement.

Scope of the Information Security Management System

The following section outlines the boundaries and requirements that form the scope of the ISMS.

Business Functions Within Scope

[List departments, business units, and functions included in the ISMS, with reasons and key information assets.]

Area	Information Assets	Reasons for inclusion
Finance	• Financial information • Payroll information	Protection of assets from a GDPR perspective and financial regulatory compliance.
	•	
	•	

Physical Locations Within Scope

[Outline the sites within the scope, such as offices, warehouses, etc]

Location	Comments
London HQ	Physical working premises for UK based staff. No onsite storage of documents or assets.

Technology Services Within Scope

[Summarise IT assets within the ISMS scope, including systems, networks, and the information they cover.]

Asset	Comments
Office 365	Used for storage of backoffice data, documents, sharepoint sites, etc. Notably manages employee performance reviews.
Laptops	All staff issued laptops

Outsourced Services Within Scope

[List any externally provided services that would be in scope]

Area	Assets	Description
Outsourced HR Function Managed by HR Today	• Employee data	Protection of assets from a GDPR perspective and financial regulatory compliance.
	•	
	•	

Risk Assessment & Treatment

[Briefly describe your approach to risk assessment and treatment, directing the reader to relevant corporate processes or ISMS methodologies. One is provided in the toolkit, if required.]

Key Policies & Procedures

[Reference key policies and standards guiding the ISMS.]

Policy / Procedure Name	Purpose
Information Security Policy	An overarching policy that outlines the organisation's position on information security, and sign-posts to sub-policies.

Document Maintenance & Distribution

Document Review and Maintenance

This document is reviewed regularly to ensure it remains relevant and effective. Reviews occur annually or when significant changes happen. The [responsible role/department] oversees the review process, and any employee can suggest revisions, subject to approval.

Document Accessibility

The document is available to all employees on [location, e.g., internal portal]. [Specify any access restrictions if applicable.]

Distribution

Distribution is controlled and monitored, provided to [list roles or departments]. [Specify any external distribution policies.]