

Information Security Management System Scope

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

[Purpose of Document 2](#_Toc171354477)

[Introduction 2](#_Toc171354478)

[Scope Statement 2](#_Toc171354479)

[Purpose of the ISMS 2](#_Toc171354480)

[Context of the Organisation 3](#_Toc171354481)

[Internal Issues 3](#_Toc171354482)

[Organisational Structure 3](#_Toc171354483)

[Business Processes 3](#_Toc171354484)

[Interested Internal Stakeholders 3](#_Toc171354485)

[External Issues 4](#_Toc171354486)

[Legal, Regulatory, and Contractual Obligations 4](#_Toc171354487)

[Technical Environment 4](#_Toc171354488)

[Market & Industry Conditions 4](#_Toc171354489)

[External Stakeholders 4](#_Toc171354490)

[Scope of the Information Security Management System 5](#_Toc171354491)

[Business Functions Within Scope 5](#_Toc171354492)

[Physical Locations Within Scope 5](#_Toc171354493)

[Technology Services Within Scope 5](#_Toc171354494)

[Outsourced Services Within Scope 6](#_Toc171354495)

[Risk Assessment & Treatment 6](#_Toc171354496)

[Key Policies & Procedures 6](#_Toc171354497)

[Document Maintenance & Distribution 6](#_Toc171354498)

[Document Review and Maintenance 6](#_Toc171354499)

[Document Accessibility 6](#_Toc171354500)

[Distribution 7](#_Toc171354501)

# Purpose of Document

This document outlines the scope of TechSolutions Inc.’s [Information Security Management System](https://en.wikipedia.org/wiki/Information_security_management) (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.

# Introduction

**TechSolutions Inc.** is a software development company specializing in cloud-based applications and services for small and medium-sized businesses. Our offerings include secure cloud storage, SaaS platforms, and data analytics tools. We prioritize data security and compliance, currently working towards ISO 27001 certification to enhance our Information Security Management System (ISMS). Our focus on innovation and customer-centric solutions helps businesses achieve their digital goals securely and efficiently.

# Scope Statement

The scope of the Information Security Management System (ISMS) at TechSolution.inc

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 TechSolution.inc, 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.

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

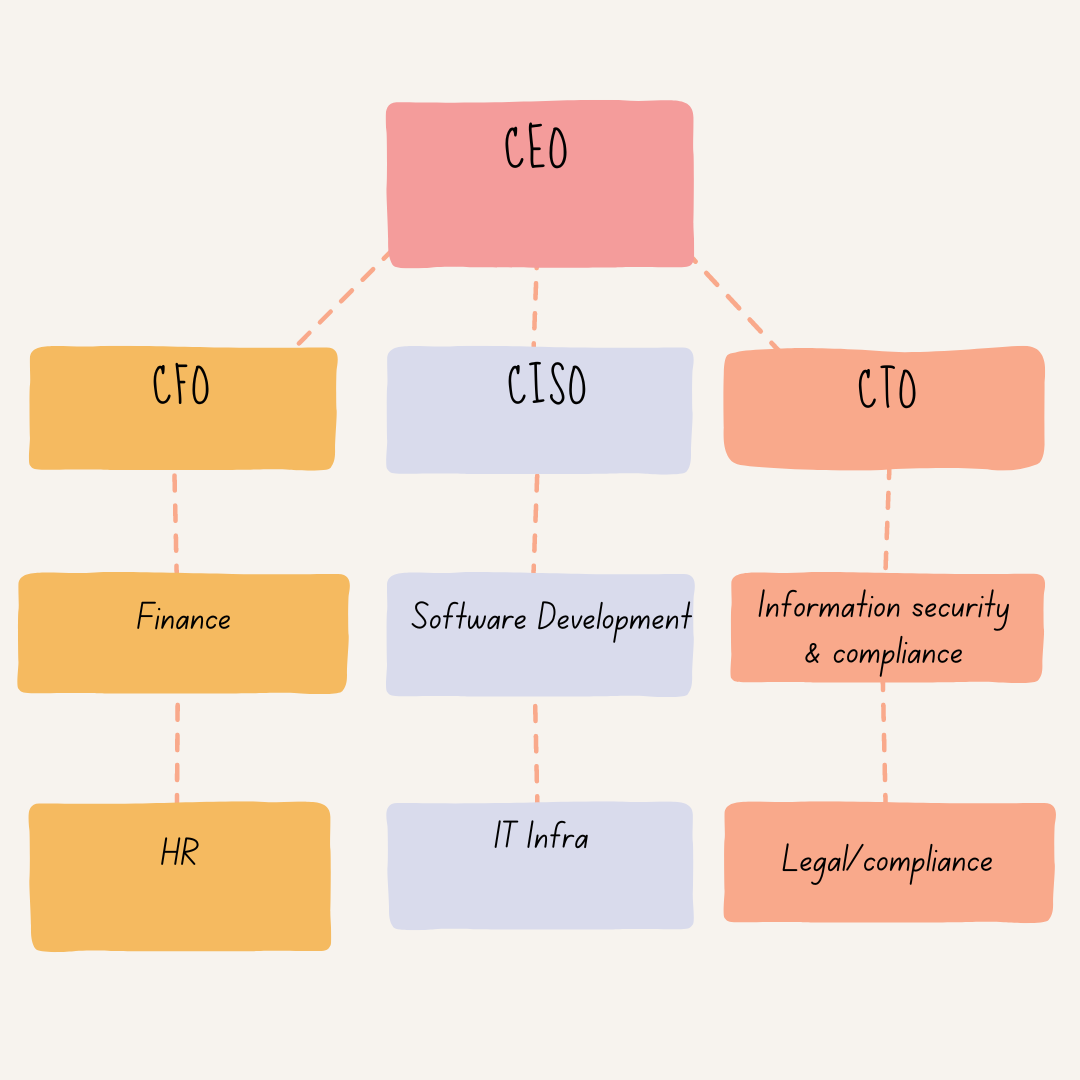
### Organisational Structure

Executive Leadership

* Chief Executive Officer (CEO): Oversees overall company strategy, growth, and operations.
* Chief Information Security Officer (CISO): Responsible for company-wide information security strategy and ensuring compliance with ISO 27001 standards.
* Chief Technology Officer (CTO): Leads the technical direction, innovation, and infrastructure of the company's software development efforts.
* Chief Financial Officer (CFO): Manages the financial health, budget, and resource allocation for all company initiatives.

2. Departments and Functions

* Information Security (IS) Department
  + Purpose: Ensures the protection of company and client data, develops security policies, and leads ISO 27001 implementation.
  + Key Roles: Security Analysts, Compliance Officers, Risk Management Team.
* Software Development Department
  + Purpose: Develops and maintains cloud-based applications and services for clients.
  + Key Roles: Software Engineers, Quality Assurance (QA) Specialists, DevOps Engineers.
* IT Infrastructure Department
  + Purpose: Manages internal and external IT systems, networks, and cloud infrastructure.
  + Key Roles: Network Administrators, System Engineers, Cloud Infrastructure Managers.
* Compliance & Legal Department
  + Purpose: Oversees regulatory compliance, risk management, and ensures legal alignment with data protection laws (GDPR, ISO 27001).
  + Key Roles: Legal Advisors, Compliance Officers.
* Sales & Marketing Department
  + Purpose: Drives customer acquisition, market outreach, and client relationship management.
  + Key Roles: Sales Executives, Marketing Specialists.
* Human Resources (HR) Department
  + Purpose: Manages recruitment, employee relations, training, and organizational development.
  + Key Roles: HR Managers, Training Coordinators.



### Business Processes

TechSolutions Inc. is a software development company specializing in providing cloud-based solutions and services to clients across various industries. The organization operates with a focus on efficiency, security, and client satisfaction. Below is a high-level overview of its major business processes:

### **1. Software Development**

* **Purpose**: To design, develop, and maintain cloud-based applications for clients.
* **Key Activities**: Requirements gathering, system design, development, testing, and deployment.
* **Security Measures**: Code reviews, version control, and secure development practices to ensure software integrity.

### **2. Customer Support**

* **Purpose**: To provide timely technical support and resolve client issues.
* **Key Activities**: Ticket management, troubleshooting, and customer feedback.
* **Security Measures**: Access control and encryption to protect customer data within support systems.

### **3. Financial Management**

* **Purpose**: To manage financial operations, including budgeting, reporting, and billing.
* **Key Activities**: Revenue tracking, expense management, and financial reporting.
* **Security Measures**: Financial data is encrypted and access is restricted to authorized personnel only.

### **4. Information Security**

* **Purpose**: To protect company and customer data through a structured Information Security Management System (ISMS).
* **Key Activities**: Risk assessments, security policy enforcement, and incident management.
* **Security Measures**: Encryption, access control, and ongoing audits following ISO 27001 standards.

### **5. IT Infrastructure Management**

* **Purpose**: To manage and maintain the company’s internal and external IT systems.
* **Key Activities**: Network management, system monitoring, and IT asset management.
* **Security Measures**: Firewalls, intrusion detection, and regular patch management to secure the infrastructure.

### **6. Compliance & Legal**

* **Purpose**: To ensure adherence to regulatory requirements and maintain legal compliance.
* **Key Activities**: Regulatory assessments, contract management, and compliance audits.
* **Security Measures**: Compliance with ISO 27001, GDPR, and other data protection regulations through regular assessments and reporting.

### Interested Internal Stakeholders

The following are the key internal stakeholders who have an active interest in Information Security within Techsolution.inc.

|  |  |
| --- | --- |
| 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

|  |  |
| --- | --- |
| 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. |

### Technical Environment

### **1. Increased Use of Cloud Computing and SaaS Solutions**

* **Impact**: TechSolutions Inc.'s reliance on cloud infrastructure for its products and services has introduced both opportunities and risks.
* **Risks**: Misconfigurations of cloud environments, insecure APIs, and unauthorized access to cloud resources have become key vulnerabilities. The **shared responsibility model** between cloud providers and TechSolutions requires stringent internal controls to manage risks effectively.

### **2. Ransomware Attacks**

* **Impact**: Ransomware has become one of the most prevalent threats across industries, including software development companies like TechSolutions.
* **Risks**: Increased instances of ransomware targeting critical infrastructure, data repositories, and customer databases. Attackers use phishing, malicious software, and vulnerabilities in remote work environments to gain access to systems.
* **Mitigation**: The company must continually improve **backup procedures**, **endpoint detection and response (EDR)**, and ensure that **employee training** on phishing and security awareness is frequent.

### **3. Supply Chain Attacks**

* **Impact**: As TechSolutions Inc. relies on third-party vendors and partners for cloud infrastructure and software components, the company faces growing risks related to supply chain attacks.
* **Risks**: Attackers may compromise third-party vendors, infiltrating systems through trusted software or hardware providers. This has been seen in high-profile incidents like the **SolarWinds breach**.
* **Mitigation**: Continuous vetting of third-party suppliers, enhanced **vendor risk management**, and regular auditing of external partnerships are required to manage these risks.

### **4. Advanced Persistent Threats (APTs)**

* **Impact**: TechSolutions’ position in the software industry makes it a target for **nation-state actors** and other sophisticated cyber attackers using APTs to infiltrate networks for long periods.
* **Risks**: APTs can lead to data exfiltration, intellectual property theft, and prolonged exposure to security breaches.
* **Mitigation**: Strengthening **network segmentation**, employing **multi-factor authentication (MFA)**, and implementing **continuous monitoring** of critical assets are essential defenses.

### **5. Remote Work and BYOD (Bring Your Own Device)**

* **Impact**: The shift to remote work has expanded TechSolutions' attack surface, with more employees accessing systems from personal devices and home networks.
* **Risks**: Unsecured home networks, unpatched devices, and weak endpoint security are vulnerable to cyberattacks, including malware and unauthorized access.
* **Mitigation**: The company should enforce **remote work policies**, deploy **virtual private networks (VPNs)**, and implement **mobile device management (MDM)** to protect sensitive information.

### **6. Phishing and Social Engineering**

* **Impact**: Phishing remains one of the most effective techniques used by cybercriminals to target organizations. TechSolutions Inc. employees, especially those in customer-facing roles, are frequently exposed to phishing attempts.
* **Risks**: Phishing attacks can lead to credential theft, malware installation, or unauthorized access to systems.
* **Mitigation**: Continuous **employee security awareness training**, simulated phishing exercises, and **email filtering** technologies are necessary to combat this growing threat.

### **Emerging Technologies**:

* **Artificial Intelligence (AI) and Machine Learning (ML)** are increasingly being integrated into security solutions for enhanced threat detection and response. While AI-driven tools offer opportunities for automation and quicker identification of risks, there are also concerns about **adversarial AI** and **AI-powered attacks**, which could manipulate algorithms or automate cyberattacks.

### Market & Industry Conditions

### **1. Increased Cyber Threat Landscape**

* **Emerging Threats**: Cybercriminals are developing more sophisticated attack methods, including ransomware, phishing, and advanced persistent threats (APTs). The frequency and severity of these attacks are on the rise, particularly targeting vulnerabilities in software development processes and cloud environments.
* **Industry Response**: Organizations are adopting advanced threat detection and response mechanisms, including machine learning and AI-based security tools, to enhance their defenses.

### **2. Shift to Cloud Computing**

* **Trend**: The migration to cloud-based solutions continues to accelerate as businesses seek scalability, flexibility, and cost-efficiency. However, this shift also brings new security challenges, such as data breaches and misconfigurations.
* **Industry Response**: Companies are increasingly implementing robust cloud security practices, such as encryption, identity and access management (IAM), and continuous monitoring to protect sensitive data stored in the cloud.

### **3. Regulatory Compliance and Data Protection Laws**

* **Trend**: Stricter data protection regulations, such as GDPR, CCPA, and HIPAA, are impacting how software companies handle data security and privacy. Compliance with these regulations is becoming critical for business continuity and customer trust.
* **Industry Response**: Organizations are investing in compliance frameworks and adopting information security management systems (ISMS) like ISO 27001 to ensure they meet regulatory requirements and mitigate risks associated with non-compliance.

### **4. Remote Work and Hybrid Environments**

* **Trend**: The increase in remote work has expanded the attack surface for organizations, making them more vulnerable to cyber threats. Employees accessing corporate resources from personal devices and home networks introduce security risks.
* **Industry Response**: Companies are implementing remote work security policies, utilizing VPNs, and enhancing endpoint security measures to protect sensitive information while enabling flexible work arrangements.

### **5. Adoption of Agile and DevSecOps Practices**

* **Trend**: The shift towards Agile development methodologies and the integration of security practices within DevOps (DevSecOps) is gaining momentum. This approach promotes continuous security integration throughout the software development lifecycle.
* **Industry Response**: Organizations are adopting automated security testing tools and incorporating security assessments early in the development process to identify and mitigate vulnerabilities more effectively.

### **6. Rise of Artificial Intelligence and Machine Learning**

* **Trend**: AI and machine learning are being utilized to enhance cybersecurity measures, providing improved threat detection, incident response, and predictive analytics.
* **Industry Response**: Software companies are integrating AI-driven security solutions to identify patterns of behavior indicative of security threats and automate responses to potential incidents.

### **7. Focus on Supply Chain Security**

* **Trend**: Supply chain attacks have become a significant concern, as attackers exploit vulnerabilities in third-party vendors and software dependencies to infiltrate organizations.
* **Industry Response**: Companies are enhancing their vendor risk management processes and conducting thorough assessments of third-party providers to ensure security compliance and reduce exposure to supply chain risks.

### External Stakeholders

The following outlines the key stakeholders outside of TechSolution.inc 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. |
| |  | | --- | | **Customer**  **Support** |  |  | | --- | |  | | * Customer data (contact details, support tickets)  |  | | --- | | * Feedback and   complaint records |  |  | | --- | |  | | * Account   management information | |  |  | | --- | |  | | Essential for service delivery and maintaining customer trust; protected under data protection regulations. |
| |  | | --- | | **IT Infrastructure** |  |  | | --- | |  | | |  | | --- | |  |  * Network configurations * Server and cloud infrastructure data | Key for maintaining system integrity and protecting against unauthorized access. |
| |  | | --- | | **Development** |  |  | | --- | |  | | Source code and repositories  Testing and deployment data  Development documentation | |  | | --- | | Protection against intellectual property  theft and ensuring secure coding  practices. |  |  | | --- | |  | |
| |  | | --- | | **Human Resources (HR)** |  |  | | --- | |  | | Employee records  Recruitment and onboarding data  Performance evaluation data | Necessary for compliance with labor laws and regulations, and ensuring data privacy. |
| |  | | --- | | **Compliance &**  **Legal** |  |  | | --- | |  | | Compliance reports  Contracts and agreements  Risk assessments and audit records | Essential for demonstrating adherence to legal and regulatory obligations. |

### 

### Physical Locations Within Scope

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

### Technology Services Within Scope

|  |  |
| --- | --- |
| 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

|  |  |  |
| --- | --- | --- |
| 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

[Risk Strategy](../../../Downloads/Risk%20Strategy.pdf)

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 ISMS documentation is available to all employees on the **internal portal**.

**Access Restrictions**:

* Access to sensitive sections of the ISMS documentation, such as incident response plans and security protocols, is restricted to authorized personnel only (e.g., IT Security Team, Compliance Officers, and Management).
* Employees must use their company credentials to log in to the internal portal, and access rights will be granted based on their role and responsibilities within the organization.
* Regular audits of access permissions will be conducted to ensure compliance with the company's information security policies.

## Distribution

The distribution of the ISMS documentation is controlled and monitored. Access is granted to the following roles and departments:

* **IT Security Team**
* **Compliance Officers**
* **Management (Executive Team)**
* **Human Resources**
* **Finance Department**
* **Development Team Leads**

#### **External Distribution Policies**

* **Non-Disclosure Agreements (NDAs)**: Any external party requesting access to ISMS documentation must sign a Non-Disclosure Agreement to protect confidential information.
* **Vendor Access**: External vendors and consultants who require access to specific ISMS documents for compliance audits or security assessments will be granted limited access, subject to approval by the CISO or designated authority.
* **Monitoring and Logging**: All access to ISMS documentation is logged for auditing purposes, ensuring accountability and tracking of who accessed what information and when.
* **Regular Review**: External access permissions will be reviewed periodically to ensure they remain appropriate and necessary.