**Cybersecurity Templates**

**Information Security Management System (ISMS) Policy**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Information Security Management System (ISMS) Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Type:** | Company Policy | **Policy Code:** | [POL‑ISMS‑001] |
| **Classification:** | [C1 – Public / C2 – Internal / C3 – Confidential] | **Version:** | [v1.0] |
| **Effective Date:** | [DD MMM YYYY] | **Next Review:** | [DD MMM YYYY] |

Contents

[1. Purpose 2](#_Toc207060308)

[2. Scope and Boundaries 2](#_Toc207060309)

[3. Policy Statement 2](#_Toc207060310)

[4. Definitions (excerpt) 3](#_Toc207060311)

[5. Context & Interested Parties 3](#_Toc207060312)

[6. Leadership, Roles & Responsibilities 3](#_Toc207060313)

[7. Risk Management 3](#_Toc207060314)

[8. Information Security Objectives & KPIs 4](#_Toc207060315)

[9. Control Framework & Statement of Applicability 4](#_Toc207060316)

[10. Asset Management & Data Classification 4](#_Toc207060317)

[11. Access Control 4](#_Toc207060318)

[12. Cryptography 5](#_Toc207060319)

[13. Physical & Environmental Security 5](#_Toc207060320)

[14. Operations Security 5](#_Toc207060321)

[15. Network & Cloud Security 5](#_Toc207060322)

[16. Secure Development & Supplier Software 5](#_Toc207060323)

[17. Information Transfer & Acceptable Use 5](#_Toc207060324)

[19. Incident & Weakness Management 6](#_Toc207060325)

[20. Business Continuity & Disaster Recovery 6](#_Toc207060326)

[25. Exceptions 7](#_Toc207060327)

[26. Enforcement 7](#_Toc207060328)

[Annex A — ISMS Scope Statement (Template) 7](#_Toc207060329)

[Annex B — Roles & RACI (Example) 7](#_Toc207060330)

[Annex C — Information Security Objectives Register (Scaffold) 8](#_Toc207060331)

[Annex D — Risk Criteria & Matrix (Template) 8](#_Toc207060332)

[Annex E — Statement of Applicability (SoA) Mapping Table 8](#_Toc207060333)

[Annex F — Incident Escalation Matrix (Template) 8](#_Toc207060334)

[Annex G — Supplier Security Checklist (Extract) 9](#_Toc207060335)

[Annex H — Definitions & Abbreviations 9](#_Toc207060336)

# Information Security Management System (ISMS) Policy

# 1. Purpose

This policy establishes the principles, governance, and mandatory requirements for [Organisation]’s ISMS to protect the confidentiality, integrity, and availability of information and to meet legal, regulatory, and contractual obligations.

# 2. Scope and Boundaries

* **Scope**—The ISMS covers the people, processes, facilities, technologies, and information assets supporting: [business services, products, functions, locations, cloud platforms].
* **In‑Scope Parties**—Employees, contractors, managed service providers, and third parties processing information on [Organisation]’s behalf.
* **Exclusions/Boundaries**—[e.g., cloud provider physical security and data‑centre environmental controls managed by the cloud provider; customer-owned environments where contractual responsibility lies with the customer]. Rationale for each exclusion must be documented in the SoA.
* **Interfaces & Dependencies**—[e.g., corporate IT, facilities, HR, legal, third‑party data centres, payment processors].

# 3. Policy Statement

[Organisation] is committed to establishing, implementing, maintaining, and continually improving an ISMS aligned to ISO/IEC 27001:2022. Leadership will ensure adequate resources, assign responsibilities, set measurable security objectives, and review ISMS performance at planned intervals.

# 4. Definitions (excerpt)

* **Information Asset**: Any data, device, system, application, or service of value to [Organisation].
* **Risk**: Effect of uncertainty on objectives.
* **Control**: Measure that modifies risk (technical, organisational, or procedural).
* **Interested Party**: Person or entity that can affect, be affected by, or perceive itself to be affected by ISMS outcomes.

(See Annex H for a complete glossary.)

# 5. Context & Interested Parties

* **Internal/External Issues**—Regulatory landscape, customer requirements, threat environment, business strategy, supply chain, and technology stack will be reviewed at least annually.
* **Interested Parties & Needs/Expectations**—Maintain a register of stakeholders (customers, regulators, employees, suppliers, and partners) and their requirements, reviewing it annually or upon significant changes.

# 6. Leadership, Roles & Responsibilities

* **Top Management**—Demonstrates commitment, approves the ISMS policy and objectives, integrates ISMS requirements into business processes, and chairs management review.
* **ISMS Manager/CISO**—Owns this policy, coordinates ISMS implementation, ensures competence, reporting, and continual improvement.
* **Information Owners / System Owners**—Classify assets, approve access, define backup and retention, and ensure control effectiveness.
* **HR**—Integrates security into hiring, onboarding, disciplinary, and termination processes.
* **All Personnel**—Comply with policies, complete training, report incidents/weaknesses promptly.
* **RACI**—See Annex B for an example RACI covering risk, SoA, incidents, change, suppliers, and audits.

# 7. Risk Management

* **Method**—Identify assets and processes; evaluate threats, vulnerabilities, likelihood, and impact using the organisation’s risk criteria (Annex D).
* **Treatment Options**—Mitigate, accept, avoid, or transfer; define treatment plans, owners, and due dates.
* **Risk Acceptance**—Residual risks must be approved by authorised risk owners within defined thresholds.
* **Risk Register**—Maintain a living register with status, review dates, and links to controls and testing evidence.

# 8. Information Security Objectives & KPIs

Set measurable objectives (e.g., training completion ≥ 98%, critical patch SLA ≤ 14 days, P1 incident MTTR ≤ 4 hours, % systems with MFA ≥ 99%). Track progress quarterly and review during the management review. (Annex C provides a register scaffold.)

# 9. Control Framework & Statement of Applicability

* **Framework**—Adopt ISO/IEC 27001 Annex A (2022) themes (e.g., organisational, people, physical, technological controls).
* **SoA**—Document included/excluded controls, justification, status, and evidence locations. Review after risk or context changes and at least annually.

# 10. Asset Management & Data Classification

* Maintain an Asset Inventory (owners, locations, criticality, data categories).
* Classify information [Public / Internal / Confidential / Restricted] and apply handling rules: storage, transmission, retention, and disposal.
* Protect records throughout their lifecycle; apply secure disposal to media and paper.

# 11. Access Control

* **Principle**—Least privilege, need‑to‑know, unique IDs; MFA for privileged and remote access.
* **Joiners/Movers/Leavers**—Time-bound approvals, periodic reviews, and immediate de-provisioning upon exit.
* **Privileged Access**—Strong authentication, session monitoring, and heightened logging; break‑glass procedures with approval and review.

# 12. Cryptography

* Use approved algorithms and key lengths; document key‑management processes (generation, rotation, escrow, revocation).
* Encrypt sensitive data at rest and in transit; consider customer-managed keys for highly sensitive workloads.

# 13. Physical & Environmental Security

* Secure facilities with access controls, visitor management, surveillance, and segregation of critical areas.
* Protect equipment from environmental threats; define clear desk/screen and secure storage requirements.

# 14. Operations Security

* **Configuration & Hardening**—Baseline standards, vulnerability management, anti-malware, logging, and time synchronisation.
* **Change Management**—Risk-based change approvals, testing, rollback, and segregation of duties.
* **Backup & Recovery**—Document RTO/RPO, test restores, and protect backups from tampering.

# 15. Network & Cloud Security

* Segment networks, protect perimeters, and apply secure remote access with VPN or ZTNA.
* Cloud controls must address identity, encryption, logging, workload protection, and shared‑responsibility boundaries.
* Prohibit unmanaged shadow IT and enforce onboarding to a central identity and monitoring system.

# 16. Secure Development & Supplier Software

* Apply secure SDLC: threat modelling, code review, dependency management, static/dynamic testing, and secure pipelines.
* Third-party components must be vetted; track SBOM for critical applications.

# 17. Information Transfer & Acceptable Use

* Use approved channels (SFTP, TLS 1.2+ APIs, managed email encryption).
* Pseudonymise or minimise data where feasible; prohibit public links for restricted data.
* Acceptable Use requirements apply to corporate systems, messaging, and collaboration tools.

**18. Supplier & Third‑Party Security**

* Risk‑rate suppliers; include privacy/security clauses, audit rights, breach notification, and sub-processor conditions.
* Maintain a supplier register; conduct periodic reassessments and evidence reviews.

# 19. Incident & Weakness Management

* Report suspected incidents immediately to [SOC / ISMS Manager] via [channel].
* Execute the Incident Response Plan: detect → contain → eradicate → recover → learn.
* Notify regulators/customers as required; maintain incident records and post‑incident actions.

# 20. Business Continuity & Disaster Recovery

* Maintain and test BCP/DR plans; define critical processes, dependencies, RTO/RPO, and recovery teams.
* Conduct exercises at least annually and after significant changes.

**21. Compliance, Legal & Privacy**

* Identify applicable laws, regulations, and contractual obligations, and monitor any changes.
* Ensure privacy by design and by default; coordinate with the DPO as applicable.
* Prohibit unauthorised software and unlawful monitoring; respect IP and licensing.

**22. Awareness & Competence**

* All personnel must complete onboarding and annual security training, as well as role-based training for elevated roles (e.g., administrators, developers, support staff).
* Keep training records and track completion KPIs.

**23. Performance Evaluation, Audit & Continuous Improvement**

* Monitor controls, KPIs, audit findings, incidents, nonconformities, and corrective actions.
* Conduct internal audits per annual plan; address nonconformities through corrective actions with owners and due dates.
* Management commits to continual improvement of the ISMS.

**24. Management Review**

Top Management shall review the ISMS at planned intervals (at least annually). Inputs include audit results, risk status, KPIs, incidents, stakeholder feedback, and opportunities for improvement; outputs include decisions on resources, objectives, and policy changes.

# 25. Exceptions

* Exceptions must be documented with a risk assessment, compensating controls, an expiry date, and approvals from [ISMS Manager] and [Executive].
* Review exceptions at least every six months.

# 26. Enforcement

Policy breaches may result in disciplinary action, up to and including termination of employment/contract, and potential legal remedies.

**Sign‑Off**

**Chief Executive Officer**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date**: \_\_\_\_\_\_\_\_\_  
**CISO / ISMS Manager**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date**: \_\_\_\_\_\_\_\_\_

# Annex A — ISMS Scope Statement (Template)

* **Organisation & Sites**: [Head office, data centres, cloud regions, remote workforce model]
* **Processes & Services**: [List critical processes/services covered]
* **Assets & Technologies**: [Platforms, applications, tooling, data types]
* **External Interfaces**: [Partners, MSPs, cloud providers, payment gateways]
* **Boundaries/Exclusions**: [Justified list with reasons]
* **Assumptions/Dependencies**: [e.g., shared responsibility with cloud provider]

# Annex B — Roles & RACI (Example)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Activity** | **Exec** | **ISMS Mgr** | **Sys Owner** | **HR** | **Legal** | **Procurement** |
| Approve Policy | A | R | C | C | C | C |
| Risk Assessment | C | R | R | C | C | C |
| SoA Maintenance | C | R | R | \_ | \_ | \_ |
| Incident Response | C | C | C | C | C | C |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| (A=Approver, R=Responsible, C=Consulted, I=Informed) |  |  |  |  |  |  |  |

# Annex C — Information Security Objectives Register (Scaffold)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Objective** | **Metric / Target** | **Baseline** | **Owner** | **Plan** | **Review Frequency** |
| e.g., Patch SLA | Critical ≤14 days | 62% | Head of IT Ops | Harden CM, auto‑patch | Monthly |

# Annex D — Risk Criteria & Matrix (Template)

* **Likelihood Scale**: [Rare…Almost Certain]
* **Impact Scale**: [Low…Severe]
* **Risk Appetite/Thresholds**: [e.g., no High residual risk without CEO sign‑off]
* **Matrix**: [5×5 grid description]
* **Treatment Triggers**: [When to mitigate, accept, escalate]

# Annex E — Statement of Applicability (SoA) Mapping Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Annex A Control (2022)** | **Included?** | **Justification** | **Implementation Summary** | **Evidence/Link** | **Status** |
|  |  |  |  |  |  |

# Annex F — Incident Escalation Matrix (Template)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Severity** | **Description** | **Initial Actions** | **Comms** | **Reg/Customer Notice** | **Approval** |
| P1 | Major impact/ data breach | Contain, IR lead engaged | Exec & Legal | Within [X] hours if required | [Roles] |

# Annex G — Supplier Security Checklist (Extract)

* Security & privacy terms in contract
* Breach notice [X] hours; sub-processor controls
* Evidence of controls (certifications, pentest, SOC reports)
* Data location, encryption, access, logging
* Exit/transition plan and data return/erasure

# Annex H — Definitions & Abbreviations

[Include terms used in this policy; align with corporate glossary.]