POLICY

Information Security Policy

The top level policy that sets direction and commitment for the ISMS

Document owner	[Owner name and role]
Approved by	[Approver name and role]
Version	[1.0]
Effective date	[Date]
Next review	[Date, at least yearly]
Classification	[Internal]

Purpose

This policy sets the direction for information security at [Company Name]. It states management's commitment, the security objectives, the roles that run the information security management system (ISMS), the approach to risk, and the set of supporting policies that staff must follow.

[Company Name] protects the confidentiality, integrity and availability of its own information and of the information customers trust it with. This policy is the reference point for every other security policy, procedure and standard.

Scope

This policy applies to:

- All employees, contractors, interns and temporary staff of [Company Name], wherever they work.
- All information created, stored, processed or sent by [Company Name], in any format.
- All systems used for company work, including cloud infrastructure in [AWS / GCP / Azure], SaaS applications, company laptops and mobile devices that access company data.
- Third parties that access company systems or data, through their contracts.

The scope of the ISMS is defined in the [ISMS Scope Statement], approved on [Date]. At the time of approval it covers [scope summary], for example the product platform, its cloud infrastructure and the teams that build, run, sell and support it.

Roles and responsibilities

Role	Responsibilities
Top management ([CEO and leadership team])	Approves this policy and the ISMS scope. Provides budget and people. Chairs or attends the management review. Accepts residual risks above the acceptance level.
[Security Lead] (ISMS owner)	Runs the ISMS day to day. Maintains policies, the risk register and the Statement of Applicability. Reports security performance to top management. Coordinates audits.
[Security Committee]	Meets [quarterly]. Reviews risks, incidents, objectives and audit results. Approves supporting policies when delegated by top management.
[IT Manager]	Operates identity, device and SaaS controls. Manages the MDM, access provisioning and the asset inventory.
[Engineering Lead]	Applies security controls in cloud infrastructure, code and deployment pipelines.
[People Operations Lead]	Runs background checks, onboarding, offboarding and the collection of policy acknowledgments.
Asset and risk owners	Classify the assets they own, approve access to them and own the treatment of related risks.
All staff	Follow this policy and supporting policies, complete security training and report incidents and weaknesses.

Policy statements

Commitment

1. Top management must approve this policy and must review it at least once every [12 months].
2. Top management must provide the resources needed to establish, operate, maintain and improve the ISMS, and must record resource decisions in management review minutes.
3. [Company Name] must meet applicable legal, regulatory and contractual security requirements, and the [Security Lead] must keep a register of these requirements.
4. [Company Name] must continually improve the ISMS based on audit results, incidents, risk reviews and feedback.

Security objectives

5. [Company Name] must set measurable security objectives each year, approved by top management. The starting objectives are:

Objective	Measure	Target
Protect accounts from takeover	Percentage of user accounts with MFA through SSO	[100%]
Keep devices secure	Percentage of company laptops compliant in the MDM (encryption, screen lock, supported OS)	[98%] or higher
Fix serious vulnerabilities quickly	Critical vulnerabilities fixed within the target time	[95%] fixed within [number] days
Build security awareness	Staff who complete annual training on time	[100%] within [30] days of assignment
Respond to incidents well	High and critical incidents with a completed lessons learned review	[100%]

6. The [Security Lead] must report progress on objectives to the [Security Committee] at least [quarterly].

Risk approach

7. [Company Name] must identify, assess and treat information security risks using the [Risk Management Procedure].
8. A full risk assessment must take place at least once every [12 months] and after significant changes, such as a new product, a major infrastructure change, an acquisition or a serious incident.
9. Every risk must have a named owner, and every risk above the acceptance level must have a treatment plan with a due date.
10. Residual risks above the acceptance level must be formally accepted by [top management], and the acceptance must be recorded.
11. The [Security Lead] must maintain a Statement of Applicability that lists the Annex A controls, whether each is applied, and the reason.

Information protection

12. Information must be classified as [Public, Internal, Confidential or Restricted] and handled according to the [Data Classification and Handling Policy].
13. Customer data must be stored only in approved systems listed in the [system inventory] and must be encrypted in transit and at rest.
14. Access to information must follow least privilege and the [Access Control Policy].
15. Staff must use company systems according to the [Acceptable Use Policy].

People

16. All staff must acknowledge this policy and the supporting policies when they join and at least once every [12 months].
17. All staff must complete security awareness training within [30] days of joining and at least once every [12 months].
18. Security responsibilities that continue after employment ends, such as confidentiality, must be stated in employment contracts or contractor agreements.

Suppliers

19. Suppliers that store or process confidential information must be assessed for security risk before contract signature and reviewed at least [annually], according to the [Supplier Security Policy].

Incidents and continuity

20. Staff must report suspected security incidents and weaknesses immediately through [#security channel / security@company email / ticketing tool].
21. Incidents must be handled according to the [Incident Response Plan].
22. Critical services must have tested backup and recovery arrangements according to the [Business Continuity and Disaster Recovery Plan].

Monitoring and improvement

23. The [Security Lead] must run an internal audit of the ISMS at least once every [12 months], performed by someone who does not audit their own work.
24. Top management must hold a management review at least once every [12 months] and record decisions and actions.
25. Nonconformities must be recorded, analyzed for root cause and corrected within agreed dates.

Policy framework

This policy is supported by the documents below. Each one has its own owner and review cycle. Adapt the list to the documents your company actually has.

Document	Owner	Purpose
[ISMS Scope Statement]	[Security Lead]	Boundaries of the ISMS
Access Control Policy	[IT Manager]	Identity, authentication and access rights
Acceptable Use Policy	[Security Lead]	Rules for staff use of devices, data and tools

Document	Owner	Purpose
Incident Response Plan	[Security Lead]	Detection, response and notification of incidents
Risk Management Procedure	[Security Lead]	How risks are assessed, treated and accepted
Risk register and Statement of Applicability	[Security Lead]	Current risks and selected controls
[Data Classification and Handling Policy]	[Security Lead]	Labels and handling rules for information
[Supplier Security Policy]	[Procurement Owner]	Security of third parties and SaaS tools
[Secure Development Policy]	[Engineering Lead]	Security in code, reviews and deployments
[Change Management Procedure]	[Engineering Lead]	Approval and testing of production changes
[Business Continuity and Disaster Recovery Plan]	[CTO]	Backups, recovery and continuity of service

Exceptions

Exceptions to this policy or any supporting policy must be requested through [ticketing tool]. Each request must describe the business reason, the risk, any compensating controls and an end date. The [Security Lead] must assess the risk, and the risk owner must approve the exception. Exceptions must not exceed [12 months] and must be recorded in the [exceptions register].

Enforcement

Violations of this policy may lead to disciplinary action, up to and including termination of employment or contract, in line with [Company Name]'s HR procedures and applicable law. Access may be suspended while a suspected violation is investigated. Compliance is checked through internal audits, technical monitoring and access reviews.

Related documents

- [ISMS Scope Statement]
- Access Control Policy
- Acceptable Use Policy

- Incident Response Plan
- Risk Management Procedure
- Risk register and Statement of Applicability

Annex A mapping

Annex A control	Section that covers it
5.1 Policies for information security	Purpose, Commitment, Review and approval
5.2 Information security roles and responsibilities	Roles and responsibilities
5.3 Segregation of duties	Monitoring and improvement (statement 23)
5.4 Management responsibilities	Commitment, People
5.12 Classification of information	Information protection (statement 12)
5.19 Information security in supplier relationships	Suppliers
5.24 Information security incident management planning and preparation	Incidents and continuity
5.31 Legal, statutory, regulatory and contractual requirements	Commitment (statement 3)
5.35 Independent review of information security	Monitoring and improvement
5.36 Compliance with policies, rules and standards for information security	Enforcement, Monitoring and improvement
6.2 Terms and conditions of employment	People (statement 18)
6.3 Information security awareness, education and training	People (statement 17)
6.4 Disciplinary process	Enforcement

This policy also supports the ISMS clauses on leadership, policy, objectives and management review.

Review and approval

The [Security Lead] must review this policy at least once every [12 months] and after significant changes to the business, the ISMS scope, the risks or legal requirements. Top management approves each new version. Approved changes are recorded in the document control table, published in [policy location] and communicated to all staff, who must acknowledge the new version within [30] days.