Information Security Management System (ISMS) Policy

This policy outlines **Unicis Tech OÜ's commitment to protecting customer data and information assets** in accordance with **ISO 27001:2022** and applicable EU regulations (GDPR, NIS2, CRA, DORA).

isms, policy, iso27001, security, information-security

Security Commitment

Unicis Tech OÜ is committed to:

- **Protecting the confidentiality, integrity, and availability** of customer data and business information
- **Complying with applicable laws and regulations** — GDPR, NIS2, CRA, DORA
- **Managing information security risks** — Systematic assessment and treatment of security threats
- **Responding rapidly to security incidents** — Detection within hours; response within SLA targets
- **Continuously improving** our security practices based on audit results and lessons learned

This commitment is endorsed by senior management and communicated to all employees and contractors working with customer data.

Scope of Information Security

Our Information Security Management System applies to:

- **Self-hosted infrastructure** — All servers, databases, applications, networking
- **Customer data** — Compliance controls, mappings, configurations, audit trails
- **Business information** — Financial records, strategic plans, employee data
- **All people** — Employees, contractors, and partners who access information
- **Third-party providers** — We assess security practices of vendors and subprocessors

Out of scope: Cloud platforms managed by vendors (AWS, Mautic, Dolibarr, GitHub, etc.) — vendors are responsible for their security.

Security Objectives

We measure our security performance against these targets:

Objective	Target	How We Measure
Incident Response	Respond to P1 security incidents within 2 hours	Incident response log
Vulnerability Management	Patch critical vulnerabilities within 7 days	Patch deployment log
Access Control	100% of access requests approved; revoke within 24h of departure	Access control log
Incident Detection	Detect suspicious activities continuously via monitoring	Security monitoring alerts

Objective	Target	How We Measure
Data Encryption	100% of customer data encrypted at rest and in transit	Encryption audit
Audit Compliance	Zero high/critical findings in annual audits	Third-party audit reports

See our Scorecard for real-time performance metrics.

Key Principles

Risk-Based Approach

We identify, assess, and manage information security risks using international best practices. See Risk Assessment Framework for our methodology.

Risks are prioritized by impact and likelihood; we focus resources on the most serious threats.

Shared Responsibility

Every person who touches customer data has a security responsibility:

- **Employees:** Follow security policies, report suspicious activity, complete annual training
- **Contractors:** Sign security agreements; follow security procedures
- **Leadership:** Allocate resources for security; review metrics regularly
- **Management:** Ensure controls are working; investigate incidents

See Accountability Chart for security roles and responsibilities.

Continuous Improvement

We continuously improve security through:

- **Annual third-party audits** — External verification that controls are working
- **Incident investigations** — Root cause analysis when issues occur
- **Metrics tracking** — Monitoring patch deployment, incident response time, access violations
- **Security awareness** — Regular training for all team members

Responsibilities

Role	Responsibility
CEO / ISMS Sponsor (Predrag)	Approve and support security policy; allocate resources; review metrics quarterly
CTO / Technical Lead (Peter)	Implement technical security controls; manage vulnerabilities; respond to security incidents
Operations Lead (Alexander)	Manage access control; support incident response; coordinate security training
All Employees	Follow security policies; report incidents; complete annual training

Regulatory Compliance

This ISMS policy helps Unicis comply with:

Regulation	How ISMS Supports It	Related Document
GDPR (EU 2016/679)	Article 32 (technical & organizational measures); Article 33 (incident notification)	Privacy Policy
NIS2 (EU 2022/2555)	Article 21 (cybersecurity measures); Article 23 (incident reporting)	NIS2 Scope
CRA (EU 2023/1230)	Security updates; incident management; product security	CRA Scope
DORA (EU 2023/2164)	Operational resilience; risk management; third-party risk	Trusted Subprocessors

Related Policies & Standards

- ISO 27001:2022 Overview — Information Security Management System
- IT Security Policy — Detailed security procedures
- Risk Assessment Framework — How we manage security risks
- Security Controls — Technical measures we implement
- ISO 20000-1:2018 — Service Management (parallel program)

Questions About Security?

Have questions about our security commitments or compliance?

→ Email us: **security@unicis.tech**

Navigation

← Trust Center | ISO 27001:2022 →

Last reviewed: October 2026 — next review: Q4 2026

isms, policy, iso27001, security, information-security, trust