Information Security Policy (summary)

DEMO DOCUMENT — Demo Cloud d.o.o. is a fictional company. This document is illustrative sample content of the IVERIOS Trust Center demo and contains no real data.

Document owner: Chief Information Security Officer · Approved by: Management Board · Version 5.0 · Effective 15 January 2026 · Review: annually

1. Purpose

Demo Cloud d.o.o. provides e-invoicing, document archive and workflow services that our customers rely on for their daily business and legal obligations. This policy sets out how we protect the confidentiality, integrity and availability of customer data and of our services. It is the top-level policy of our information security management system (ISMS), certified to ISO/IEC 27001:2022.

2. Commitments of the Management Board

- Information security is a board-level responsibility. The CISO reports directly to the CEO and presents the security status to the board every quarter.
- We comply with applicable law and contracts, including GDPR, the Croatian Cybersecurity Act (NIS2), DORA requirements of our financial-sector customers and the Fiscalization Act.
- We set measurable security objectives every year and provide the resources needed to achieve them.
- We continually improve the ISMS through risk assessment, internal audits, management reviews and lessons learned from incidents and tests.

3. Principles

- Risk-based approach — assets and suppliers are assessed at least yearly; risks above appetite require an approved treatment plan.
- Least privilege and need to know — no standing access to customer data; access is granted just in time, approved and logged.
- Security by design — threat modelling, secure coding (OWASP ASVS level 2), peer review and automated security testing for every change.
- Encryption everywhere — TLS 1.2+ in transit, AES-256 at rest, keys in hardware-backed key management.
- EU data residency — customer data is stored and processed only in the European Union.
- Resilience — redundancy across availability zones, tested backups and a disaster recovery plan with RPO 15 minutes and RTO 4 hours.
- Transparency — customers are informed of personal data breaches within 24 hours of confirmation.

4. Supporting policies

Acceptable use · Access control · Cryptography · Secure development · Change management · Logging and monitoring · Vulnerability management · Supplier security · Incident management · Business continuity and disaster recovery · Data classification and retention · Human resources security · Physical security · AI use.

5. Responsibilities

All employees and contractors must comply with this policy and its supporting policies, complete security training at onboarding and annually, and report security events immediately to security@demo-cloud.example. Violations are handled under the disciplinary process.

DEMO DOCUMENT: Demo Cloud d.o.o. is a fictional company. This policy is illustrative sample content of the IVERIOS Trust Center demo.

DEMO