MarkAIting Pro – Corporate Information Security Policy

Version 1.0 – Approved by the Executive Board on 2025-06-12

1 Introduction

MarkAIting Pro ("the Company") is committed to safeguarding the confidentiality, integrity and availability of all information assets entrusted to us by clients, partners and employees. This Security Policy defines the minimum controls required to protect information throughout its life-cycle, in compliance with ISO 27001 principles and applicable data-protection laws.

2 Purpose

This document establishes directives and responsibilities for:

1. Assessing and managing information-security risk;
2. Implementing appropriate technical and organisational controls;
3. Ensuring timely detection, response and recovery from security incidents.

3 Scope

The policy applies to **100 %** of MarkAIting Pro's personnel, contractors and third parties who create, access or process Company information, whether on-site or remotely.

4 Roles & Responsibilities

Role	Key Security Duties
Chief Information Security Officer (CISO)	Owns this policy; chairs monthly risk review.
Department Managers	Enforce controls within their teams; report deviations within **24 h**.

All Employees	Comply with the controls; complete annual training (minimum score **85 %**).

5 Core Security Controls

5.1 Access Management

1. **Least privilege**: users receive only the minimum rights needed.
2. **Multi-factor authentication (MFA)** is mandatory for all cloud and VPN logins.
3. Accounts inactive for **90 days** are automatically disabled.

5.2 Asset Protection

1. Laptops must employ full-disk AES-256 encryption.
2. Confidential data at rest in the cloud storage must be encrypted with keys rotated every **365 days**.
3. Removable media is prohibited unless approved by the CISO.

5.3 Network Security

1. Office Wi-Fi uses WPA3-Enterprise; guest network is isolated VLAN.
2. All inbound ports except **443** and **22 (SSH-bastion only)** are blocked by default.
3. Quarterly penetration tests are conducted; critical findings (CVSS ≥ 9.0) fixed within **14 days**.

5.4 Secure Development

1. Source code repositories use branch protection & signed commits.
2. Static security scans run on every pull request with ≤ **1** high-severity issue permitted.
3. Secrets must be stored in a managed vault—never in plain-text config.

6 Incident Response

1. All employees must report suspected incidents to security@markaiting.pro within **15 minutes**.
2. The CISO coordinates the Incident Response Team (IRT) to contain, eradicate and recover.
3. Post-incident review is held within **5 business days**, generating a corrective-action plan.

7 Compliance & Audit

- The Company aligns with **GDPR**, **CCPA** and **ISO 27001** controls A.5–A.18.
- Internal audits occur twice per year; external audits annually.

8 Enforcement

Policy violations may lead to disciplinary action up to and including termination and legal prosecution.

9 Policy Review

This document is reviewed at least **once every 12 months** or upon significant business/technology change.

Document owner: CISO | Next review: 2026-06-12