ENS Information Security Policy: Corsano B.V.

Sign off	
	
Author: Jelmer Nieuwenhuis **Date**: 19-03-2026	**Approver**: Peter Stas **Date**: 07-04-2026

Revision	Date	Record of Changes	Author	Approved By
1.0	02-04-2026	Initial issue	Jelmer Nieuwenhuis	Peter Stas

1. Objectives and Mission (Art. 12.1.a)

The mission of Corsano B.V. is to provide a world-class, professional health monitoring environment through the Corsano Health Monitoring Platform. Our primary objective is to manage processes impacting information security with the highest level of readiness and quality. We are committed to ensuring transparency for our customers and stakeholders by safeguarding the availability, integrity, and confidentiality of all processed data.

2. Regulatory Framework (Art. 12.1.b)

Corsano B.V. operates within a robust legal and regulatory framework. Our Information Security Management System (ISMS) is designed to comply with:

- **ENS (Esquema Nacional de Seguridad):** Category MEDIUM/HIGH.
- **ISO 27001:2022 & NEN 7510-1:2024:** For general and healthcare-specific information security.
- **HDS (Hébergeur de Données de Santé):** For French healthcare data hosting requirements.
- **ACN Cloud Qualification:** Level 3 / QC3 (Italy).
- **BSI C5:2020:** For cloud service security criteria.

3. Security Roles and Responsibilities (Art. 12.1.c)

To ensure accountability, Corsano B.V. defines the following roles:

- **Management Board:** Responsible for approving the policy, aligning it with strategic goals, and providing necessary resources.
- **Chief Information Security Officer (CISO):** Responsible for the implementation, maintenance, and continuous improvement of the ISMS.
- **System Administrators:** Responsible for the technical execution of security controls and system integrity.
- **Employees:** Responsible for applying ISMS documentation consistently and reporting security incidents.

- **Appointment:** Roles are appointed by Management based on professional competence. Responsibilities are reviewed annually or upon significant organizational changes.

4. Security Management and Coordination Committee (Art. 12.1.d)

Corsano has establis**h**ed a Security Management Committee consisting of leadership and technical security leads.

- **Responsibility:** This committee oversees risk management, approves security initiatives, and ensures that security is integrated into all business processes.
- **Coordination:** It acts as the liaison between technical operations and executive management, ensuring that security objectives align with the organization's context.

5. Security Documentation Structure (Art. 12.1.e)

The security documentation is managed through a structured hierarchy to ensure clarity and controlled access:

- **Level 1: ISMS Policy (This Document):** High-level objectives and principles.
- **Level 2: Procedures & Standards:** Detailed "how-to" guides for security processes.
- **Level 3: Records & Logs:** Evidence of control effectiveness (e.g., audit logs, incident reports).
- **Management:** Documentation is stored in a secure, central repository. Access is granted based on the "need-to-know" principle.

6. Risks from Processing Personal Data (Art. 12.1.f)

Given the processing of sensitive health data, Corsano B.V. conducts specific risk assessments regarding the rights and freedoms of data subjects. These assessments are aligned with the **ENS Medium/High** requirements to mitigate threats such as unauthorized access, data loss, or breaches of medical confidentiality.

7. Minimum Security Requirements (Art. 12.6)

Corsano B.V. implements the following minimum requirements in proportion to the identified risks:

- **Risk Management:** Continuous risk analysis serves as the foundation for all security measures.
- **Personnel Management:** Employees are trained and made aware of their duties regarding security and legal regulations.
- **Access Control:** Strict authorization based on the **Principle of Least Privilege** (Art. 12.6.h).
- **System Integrity:** Regular updates, activity logging, and detection of harmful code (Art. 12.6.i, l).
- **Information Protection:** Security of data at rest and in transit (Art. 12.6.j).
- **Business Continuity:** Strategies are in place to ensure the persistence of the Health Monitoring Platform during disruptions.
- **Continuous Improvement:** Management is committed to maintaining and improving the ISMS through regular audits and KPI monitoring.