

Information Security Statement for Customers

Version: 1.0

Date: September 2026

Author: Senseca Group | Global Communications

1. Our Commitment to Information Security

Information is one of the most valuable assets of every organization. The protection of customer information, intellectual property, business processes and IT systems is therefore an integral part of Senseca Group's corporate governance.

As an international technology company, we continuously develop our information security capabilities to address evolving cyber threats, regulatory requirements and customer expectations. Our objective is to maintain an appropriate level of protection for the confidentiality, integrity and availability of all information entrusted to us.

2. Our Information Security Management System

Senseca Group is implementing and continuously improving a structured **Information Security Management System (ISMS)**. Our ISMS follows a risk-based approach and is aligned with the principles of internationally recognized information security frameworks and applicable regulatory requirements, including the European **NIS2 Directive** and its national implementations where applicable.

Information security is treated as an ongoing management process.

This includes:

- Information Security Governance
- Management Commitment
- Defined Roles and Responsibilities
- Information Security Policies
- Risk Management
- Business Continuity Management
- Incident Management
- Supplier Security Management
- Document Management
- Continuous Improvement

Executive management regularly reviews the effectiveness of these measures and defines priorities for further development.

2.1 Cyber Resilience Act (CRA) Readiness

Senseca Group recognizes the importance of the European **Cyber Resilience Act** (CRA) and its role in strengthening cybersecurity requirements for products with digital elements.

As part of our ongoing information security and compliance program, Senseca Group is actively assessing the applicable CRA requirements and implementing the necessary organizational, technical and governance measures.

The implementation follows the regulatory timeline of the CRA:

- **By 11 September 2026:** Senseca will establish the organizational processes required to support the CRA reporting obligations for actively exploited vulnerabilities and severe security incidents affecting products with digital elements.
- **During 2026 and 2027:** Senseca will continue assessing and strengthening relevant product-security processes, including secure development, vulnerability management, product lifecycle management, security documentation and supporting governance structures.
- **By 11 December 2027:** Senseca aims to have the relevant processes, controls and documentation in place to meet the main CRA obligations applicable to products with digital elements within the relevant scope.

Our CRA readiness activities include:

- Assessment of applicable CRA requirements and affected products
- Review and enhancement of secure development and product lifecycle processes
- Development of vulnerability management, monitoring and coordinated disclosure processes
- Assessment of software, firmware and third-party component dependencies
- Evaluation and improvement of product security documentation and evidence
- Integration of relevant CRA requirements into existing governance and management processes
- Continuous monitoring of regulatory guidance and implementation requirements

Senseca follows a risk-based and proportionate implementation approach, prioritizing legally required measures and product-security controls based on product scope, risk, customer requirements and regulatory applicability.

By integrating CRA-related requirements into our broader management framework, Senseca aims to establish a sustainable product-security approach and further strengthen transparency and customer confidence.

3. Our Security Measures

As part of our ongoing information security improvement program, the following organizational and technical foundations have been established and are continuously maintained.

3.1 Organizational Controls

To provide an appropriate level of information security, Senseca Group has established documented organizational controls including:

- Information Security Policies
- Defined Security Responsibilities
- Risk Assessments
- Business Continuity Planning
- Emergency Procedures
- Incident Response Processes
- Supplier Security Management
- Management Reviews
- Information Security Awareness and Training

These measures and related documentation are reviewed regularly and updated whenever necessary.

3.2 Technical Security

Technical controls are implemented and maintained in accordance with defined security baselines. Where appropriate, this includes multi-factor authentication for privileged and remote access, encryption of sensitive data in transit and at rest, and risk-based vulnerability and patch management aligned with the criticality of identified vulnerabilities.

Examples include:

- Role-based Access Control
- Secure Authentication Mechanisms
- Vulnerability and Patch Management Process
- Backup and Recovery Procedures
- Technical Security Assessments
- Network and System Documentation
- Asset Management
- Change Management
- Continuous Monitoring of Security-relevant Systems and Events

3.3 Supplier Security

Information security extends beyond organizational boundaries. Suppliers with a security-relevant impact are evaluated using a documented assessment process. The assessment includes topics such as:

- Organizational Security
- Technical Security
- Data Protection
- Business Continuity
- Security Certifications
- Contractual Requirements
- Criticality of Supplied Services

3.4 Business Continuity Management

Maintaining business operations is an essential part of our security strategy. Critical business processes are analyzed to determine their protection requirements and appropriate continuity measures. Business Continuity Plans and emergency procedures are regularly reviewed and continuously improved.

4. Working Together with Our Customers

Information security is a shared responsibility between Senseca Group and its customers. Where appropriate and contractually agreed, we provide relevant information regarding our information security management approach and support customer-specific security requirements throughout our business relationship.

5. Our Commitment

Senseca Group is committed to continuously strengthening its Information Security Management System.

Our objective is to:

- Protect Customer Information
- Reduce Cyber Risks
- Strengthen Business Resilience
- Comply with Applicable Legal and Contractual Requirements
- Continuously Improve our Security Capabilities
- Remain a Trusted and Reliable Business Partner for Our Customers

Our security and compliance programs consider relevant legal and regulatory frameworks, including data protection laws, sector-specific requirements and, where applicable, the European NIS2 Directive and its national implementations. Security controls and implementation priorities



may evolve based on risk assessments, business requirements, technological developments and regulatory obligations.

Information security is not a one-time initiative; it is an ongoing management responsibility and an integral part of our corporate culture.

A handwritten signature in blue ink, appearing to read "Tom Vorwerk".

Tom Vorwerk
Vice President Global Sales

A handwritten signature in blue ink, appearing to read "Nils Strauch".

Nils Strauch
CFO