BARIX

Cybersecurity Governance and Regulatory Alignment Statement

Purpose

This statement summarizes the Company's cybersecurity governance framework, regulatory posture, and continual improvement program. It is intended to provide customers, suppliers, partners, auditors, and other interested parties with a concise overview of the Company's approach to cybersecurity, secure product development, risk management, and regulatory alignment.

Regulatory Position

The Company periodically evaluates the legislation, regulations, and industry standards applicable to its business activities, products, and services.

Based on its current assessment:

Barix AG is a company incorporated in Switzerland and obeys the Swiss Cyber Security laws. Particularly with regard to:

1. **Federal Information Security Act — Informationssicherheitsgesetz, ISG; SR 128**, particularly Articles 74a–74h.
2. **Cybersecurity Ordinance — Cybersicherheitsverordnung, CSV**
3. **Federal Data Protection Act — Datenschutzgesetz, DSG**, particularly Article 24 for personal-data breaches.
4. **The ISG/CSV Cyberattack-Reporting Obligation** took effect on 1 April 2025. Covered organisations must make an initial report to the **Swiss National Cyber Security Centre, NCSC/BACS**, within 24 hours after discovering a reportable cyberattack. Missing information may be added within 14 days.

- The Company recognizes that customers operating in regulated sectors may themselves be subject to cybersecurity legislation and may impose contractual cybersecurity and assurance requirements on their suppliers.
- Products placed on the European Union market may be subject to the requirements of the EU Cyber Resilience Act (CRA). The Company is actively implementing the governance, secure development, vulnerability management, and product lifecycle processes necessary to support compliance with applicable CRA requirements.

Integrated Governance Program

The Company maintains an integrated governance program that is continually developed and improved with the objective of aligning its policies, procedures, technical controls, product development practices, and management processes with internationally recognized standards and applicable regulatory requirements.

BARIX

The Company's governance program is based upon the principles of continual improvement, risk-based decision making, documented management systems, and secure product lifecycle management.

Alignment with Standards and Regulatory Frameworks

The Company's governance program is actively developed with reference to the following standards and regulatory frameworks, as applicable to its business activities:

- **ISO/IEC 27001** – Information Security Management Systems
- **ISO 9001** – Quality Management Systems
- **ISO/IEC 42001** – Artificial Intelligence Management Systems
- **EU Cyber Resilience Act (CRA)** (this only applies to products listed under NEW PRODUCTS, Products listed under LEGACY PRODUCTS to will not comply with CRA and will not be sold in the EU after December 11. 2027)
- Security and governance principles reflected in the **NIS2 Directive**
- **IEC 62443-4-1 and IEC 62443-4-2** — In developing our products to meet the CRA's essential cybersecurity requirements by 11 December 2027, our secure development lifecycle and component security architecture are aligned with these standards, which are being adapted through EU standardization processes to align with the CRA.

The Company periodically evaluates its level of alignment with these standards and frameworks, identifies opportunities for improvement, and implements corrective actions where appropriate. References to these standards and regulatory frameworks describe the Company's governance objectives and alignment activities. Unless expressly stated elsewhere, they should not be interpreted as claims of third-party certification, formal conformity assessment, or legal determination of regulatory status.

Cybersecurity Governance

The Company's cybersecurity program includes, where appropriate to its business activities and risk profile:

- Information security governance and documented policies.
- Risk assessment and risk treatment.
- Secure software, firmware, and product development practices.
- Secure product architecture and lifecycle management.
- Vulnerability management and coordinated vulnerability disclosure.
- Security testing, including vulnerability assessments and penetration testing appropriate to business risk.
- Security incident detection, response, investigation, corrective action, and continual improvement.
- Configuration management and controlled change management.
- Supplier and third-party cybersecurity risk management.
- Security logging, monitoring, and event investigation.
- Business continuity and disaster recovery planning.
- Personnel security awareness and cybersecurity training.
- Management review of cybersecurity risks, governance effectiveness, and continual improvement activities.

BARIX

Integrated Management System

The Company seeks to maintain a single, **Integrated Security Management System (ISMS)** that supports multiple governance objectives rather than implementing independent compliance programs for each individual standard or regulation. Where practical, common governance processes—including risk management, document control, change management, incident management, corrective action, internal review, management oversight, and continual improvement—are designed to support multiple standards and regulatory frameworks simultaneously. This integrated approach promotes consistency, reduces unnecessary duplication, and supports efficient governance across the Company's products, services, and business operations.

Continual Improvement

Cybersecurity, product security, quality management, and AI governance are treated as ongoing management disciplines. The Company continually reviews evolving threats, customer expectations, applicable legislation, recognized standards, and industry good practice. Where opportunities for improvement are identified, policies, procedures, technical controls, and management processes are updated accordingly. The Company also periodically reassesses its regulatory obligations and alignment objectives as its products, services, technologies, markets, and organizational structure evolve.

Review

This statement is reviewed periodically and updated as necessary to reflect changes in the Company's governance program, business activities, products, services, applicable legislation, standards, or organizational objectives.

Zug, 7. Sept 2026

Reto Brader CEO