Siegfried Information Security Policy

Information and cyber security represent a fundamental field of action for the entire pharmaceutical industry, as they are handling sensitive customer and patient related data.

In particular, Siegfried – as a Contract Development and Manufacturing Organization (CDMO) – handles intellectual property related to production processes and products, owned by strategic customers or by Siegfried. A leak of such information would harm our strategic partners and threaten Siegfried's reputation as a reliable partner to the pharmaceutical industry as well as diminish competitive advantages arising from know-how that was built up in Siegfried's more than 150 years of experience.

For these reasons, Siegfried has established an ISM-board (Information Security Management) and is fully committed to protecting and securely handling any information that is under control of Siegfried. This Policy applies to all Siegfried entities.

Our Information Security Vision:

Create a resilient, proactive, and adaptive information security environment that safeguards the information of Siegfried and its customers (incl. personal data) while enabling business objectives as a trusted partner.

Strategic Objectives

Protect:
Safeguard the confidentiality, availability, and integrity of data.

Support Business Resilience:
Ensure continuity of operations and risk preparedness.

Drive Continuous Improvement:
Advance our information security capabilities through proactive management and innovation.

Information Security Pillar

Governance:
- Information Security Management Board
- Information Security Management System

People
- Awareness & Training

Technology & Processes
- Incident Management
- Third-Party Risk Managementt

Governance & Framework

- The Siegfried Information Security Management System (ISMS) is aligned with ISO/IEC 27001.
- The Siegfried Information Security Management Board oversees the implementation of the strategy.
- Leadership Commitment: Executive management reviews and approves security objectives, ensuring alignment with corporate strategy and compliance priorities.

Roles & Responsibilities

- Board of Directors and Executive Committee have ultimate responsibility for information security and ensure that any information security measures are consistent with business objectives.
- Employees are responsible for implementing and maintaining information security and for protecting Siegfried information (incl. information of Siegfried's customers).
- Employees, contractors, and partners must report any suspected or confirmed incidents immediately through designated channels such as email, phone, and an internal portal. Quick and accurate reporting can mitigate the impact of security incidents.

Continuous Improvement

Siegfried continuously enhances its information security through:

- Monitoring emerging threats, regulatory changes, and technology trends.
- Annual reassessment of security objectives and controls.

Through a culture of vigilance, accountability, and innovation, Siegfried ensures that information and cyber security remain integral to our operations. Our goal is to safeguard data, protect our partners' trust, and strengthen resilience across all aspects of our business.

Siegfried Information Security Policy
Edition 2026

Issued by
Siegfried Holding AG
Siegfried Information Security Board
Edition 2026

Contact
Siegfried Holding AG
Untere Brühlstrasse 4
4800 Zofingen, Switzerland
Phone +41 62 746 11 11
www.siegfried.ch