Cybersecurity Statement – Optiprint AG

At Optiprint AG, safeguarding our information assets is a top priority. Our cybersecurity program is built on a risk-based approach that aligns with internationally recognized standards, including the German BSI-Standard 200-2 “IT-Grundschutz” and the US “Cybersecurity Maturity Model Certification” (CMMC) 2.0 methodology.

Framework & Compliance

- **BSI-Standard 200 (IT-Grundschutz):**
  We have implemented an Information Security Management System (ISMS) structured according to the BSI 200-2 methodology. This approach ensures systematic risk identification, threat assessment, and the application of tailored security measures across all organizational processes. Our ISMS integrates both, preventive and reactive controls to manage risks, maintain continuity, and continuously improve our overall security.

- **CMMC 2.0 Level 1 & 2:**
  We adhere to the foundational practices of CMMC Level 1 and the advanced safeguards of Level 2. Level 1 focuses on basic practices, such as limiting system access and ensuring basic system hygiene. While Level 2, which mirrors NIST SP 800-171, ensures comprehensive, documented processes to protect sensitive data.

- **International Framework Monitoring:**
  In today’s global environment, we recognize that cybersecurity threats and regulatory requirements extend beyond national borders. We continually review and assess cybersecurity frameworks and standards from other countries and regions. This includes, for example, ISO 27001 and the UK’s Cyber Essentials.

- **Certification:**
  We are currently not yet certified to these standards, but we are already compliant with most of the requirements. Open actions are noted in the Plan of Action & Milestones (PoA&M).

Security Measures

- **Technical Controls:**
  • Robust access control policies and multifactor authentication to restrict system access.
  • Continuous monitoring and audit logging to detect and remediate threats in real time.

Optiprint AG
Auerstrasse 37 CH-9442 Berneck Switzerland
Phone +41 71 747 86 86 www.optiprint.ch

• Secure configuration management and encryption techniques to protect data in transit and at rest where needed.

- **Administrative Controls:**
  • A comprehensive cybersecurity policy, regularly reviewed and updated, ensuring alignment with regulatory requirements and industry best practices.
  • Regular security training and awareness programs for all employees.
  • Formal risk assessments and the use of a Plan of Action & Milestones (PoA&M) to address any gaps identified in our security measures.

- **Physical Controls:**
  • Secure facilities with controlled access and environmental safeguards to protect our critical infrastructure.
  • Regular testing of backup and disaster recovery plans to ensure seamless business continuity.

- **Data Protection Commitment:**
  In addition to protecting internal information and complying with legal requirements, we are fully committed to safeguard our customer data. We implement strict access controls and continuous monitoring to ensure that customer data remains confidential, integral, and available.

Commitment to continuous Improvement

Optiprint AG is dedicated to maintaining and enhancing our cybersecurity framework. We conduct regular self-assessments, and, where applicable, third-party assessments, to ensure that our practices not only meet but exceed baseline requirements. Our commitment to cybersecurity extends to ongoing investments in technology, staff training, and process optimization to adapt to emerging threats and evolving compliance standards.

Berneck, 2025-03-03

Hansjörg Etter

CEO

Jason Deane

CISO