Information security at a glance

heidelbergmaterials.com

Heidelberg Materials

This document provides a concise overview of Heidelberg Materials' information security governance, policies, and management practices. For full details, see our Annual and Sustainability Report 2025 (ASR 2025).

01. Information Security Governance

The Supervisory Board and its Audit Committee oversight: The Audit Committee of the Supervisory Board exercises formal oversight of the Group's cybersecurity posture. On a quarterly basis, the Committee reviews the Group's risk profile, current threat landscape, and progress on mitigation measures. These discussions focus on emerging cyber risks, the status of strategic security initiatives, and the outcomes of internal and external audits. (ASR 2025, p. 16, *Internal Governance Procedures*)

Board-level oversight: Group Security provides regular updates on the cybersecurity situation to the Managing Board, the Supervisory Board, and country management. Executive accountability for IT and OT security rests with the Chief Digital Officer, Dennis Lentz, a member of the Managing Board. (ASR 2025, p. 75)

Executive Accountability: Overall responsibility for cybersecurity and resilience lies with the Group Chief Information Security Officer (CISO), Mathias Bücherl, who has led the global cybersecurity and resilience strategy since March 2023. Reporting directly to the Managing Board, the CISO delivers regular briefings to ensure that cyber resilience is fully embedded in corporate strategy and digitalisation initiatives.
(ASR 2025, p. 75, Mathias Bücherl)

Organisational structure (Three Lines of Defence):

- 1st line: Local IT security officers in all major countries (expanded in 2025 to Poland, Morocco, Thailand, Egypt, Ghana, Tanzania, and others) (ASR 2025, p. 76)
- 2nd line: Group Security — responsible for globally applicable IT security guidelines, monitoring, compliance, and implementation (ASR 2025, p. 76)
- 3rd line: Group Internal Audit — checks compliance with IT security guidelines at regular intervals (ASR 2025, p. 76)

Certifications & frameworks: ISO 27001 certification was successfully re confirmed in the first quarter of 2025 following an external IT security audit. In parallel, the Group has achieved global alignment with the NIST Cybersecurity Framework 2.0 across all countries. Compliance with the framework has been validated by an external partner. (ASR 2025, p. 75)

02. Information Security Policy

Our Information Security Policy is designed to ensure the confidentiality, integrity, and protection of data throughout its entire lifecycle.

Regulatory compliance: In response to evolving regulatory requirements, Heidelberg Materials launched a NIS2 implementation program for Europe in 2024, which continues through 2025. The program aligns technical and organisational security measures with applicable national implementing acts across European countries.
(ASR 2025, p. 76)

Secure software development: In 2025, Heidelberg Materials established a Group wide guideline for the secure development of software products. This guideline builds on automated security analysis procedures that have been in place since 2023, further strengthening secure by design principles across the Group.
(ASR 2025, p. 75)

Data protection: A comprehensive Framework Data Protection Policy applies globally. Compliance is monitored through regular internal controls and audits, with results reported to the Managing Board. Oversight is ensured by the Group Data Protection Officer, supported by local Data Protection Coordinators in each country.
(ASR 2025, p. 190)

Employee responsibilities: The Code of Business Conduct requires all Managing Board members and employees to handle company information, business secrets, and personal data with care and responsibility. This obligation is reinforced through mandatory, regular online training. With more than 48,000 employees worldwide, our workforce represents a critical line of defence against cyber threats. We promote a culture of shared responsibility through a comprehensive "Human Firewall" program.

- Mandatory Training: All employees with access to IT systems are required to complete annual, multi-language Security Awareness Training. Completion rates are systematically monitored and reported as a key performance indicator (KPI).
- Active Simulation: A continuous phishing simulation program is in place to assess organisational resilience. Insights from these simulations are used to deliver targeted, just in time education to higher risk user groups, significantly reducing susceptibility

to social engineering attacks.
(ASR 2025, p. 18, p. 76)
- Security Community: The Global Security Community is used for regular and ad hoc communications, including awareness campaigns, security alerts, knowledge sharing, and the collection of feedback and improvement ideas.

Third-party security requirements: All third-party IT service providers and cloud service operators must comply with Heidelberg Materials' information security requirements. Cloud services and outsourced IT infrastructure are assessed and continuously monitored by the Group Security team. Vendor security assessments form an integral part of the procurement process, while the Heidelberg Materials Security Operations Centre conducts ongoing third-party security monitoring using a threat intelligence platform.

03. Information Security Management

Continuous improvement: Heidelberg Materials follows a structured, continuous improvement cycle to strengthen its information security posture and resilience:

- **2023:** Launch of the NIST compliance programme and implementation of automated software security analysis procedures (ASR 2025, p. 75)
- **2024:** Achievement of ISO 27001 certification and initiation of the NIS2 implementation programme for European operations (ASR 2025, pp. 75–76)
- **2025:**
  - Successful re confirmation of ISO 27001 through an external audit
  - Group wide NIST Cybersecurity Framework (CSF) 2.0 compliance review of all IT departments, demonstrating improved maturity levels
  - Comprehensive revamp of the OT risk management process, including an end-to-end security review and risk analysis of the digital platform
  - Introduction of a new Group wide guideline for secure software development
  (ASR 2025, pp. 75–76)

Monitoring & threat response: Heidelberg Materials maintains a robust, multi layered monitoring and response capability:

- A **24/7 Security Operations Centre (SOC)** continuously monitors all critical and sensitive IT systems (ASR 2025, p. 75)
- A centralized **SIEM platform** (Security Information and Event Management) platform is used to detect, record, and manage potential security incidents (ASR 2025, p. 75)
- **Endpoint detection and response (EDR)** solutions are deployed across IT and OT environments; in 2025, legacy OT antivirus solutions were fully replaced with modern EDR technology (ASR 2025, pp. 75–76)
- The **MITRE ATT&CK framework** is used to systematically enhance defensive capabilities against cyber attacks (ASR 2025, p. 76)
- A **Threat intelligence platform** was fully integrated in 2025 to support proactive detection and response (ASR 2025, p. 76)

Business continuity: In 2025, Heidelberg Materials launched a Group-wide **Business Resilience program** that integrates:

- Business continuity management
- IT service continuity
- IT disaster recovery
- Crisis management
- Business impact analysis

The program enables rapid response and recovery in the event of disruptions. Data centres are operated across Europe, Asia, and North America, supported by standardized infrastructure, redundancy concepts, and robust backup procedures. (ASR 2025, p. 75)

Vulnerability analysis: Heidelberg Materials applies a proactive approach to identifying and remediating vulnerabilities:

- Regular automated vulnerability scans and penetration testing are performed across IT and OT environments (ASR 2025, p. 75)
- In FY 2025, four penetration tests were conducted by specialised third party providers.
- Automated security analysis of internally developed software has been in place since 2023 (ASR 2025, p. 75)
- A comprehensive OT security review and risk analysis of the digital platform was completed in 2025 (ASR 2025, p. 75)

The focus remains on early detection and timely remediation of identified vulnerabilities.

Escalation & incident reporting for employees: Heidelberg Materials maintains clear and accessible escalation and reporting channels:

- The SpeakUp whistleblower system is available to all employees and external stakeholders for reporting incidents, including anonymously. (ASR 2025, p. 189)
- A dedicated information security incident reporting process allows employees to report security incidents, vulnerabilities, or suspicious activities via a 24/7 Security Hotline, in addition to SpeakUp.

- All reports are triaged by the SOC and escalated based on a defined severity classification. (ASR 2025, p. 75)

Disclosure of breaches: In FY 2025, Heidelberg Materials recorded **no information security breaches**. Consequently, no breaches with material financial or operational impact were identified.

Heidelberg Materials AG
Berliner Strasse 6
69120 Heidelberg
Germany
heidelbergmaterials.com