MONCLER
GROUP

INFORMATION SECURITY MANAGEMENT APPROACH

Governance

The Group has established a specific governance structure to effectively manage cybersecurity-related matters.

At Board level, the oversight of the cybersecurity strategy is entrusted to the Control Risks and Sustainability Committee — a Board Committee composed of members of the Board of Directors. This Committee receives regular updates on cybersecurity (at least every six months) from the Information & Technology Transformation department and reports this information to the Board of Directors.

The Information & Technology Transformation department operates within the Corporate and Supply division, which is led by Executive Director and Group Chief Corporate & Supply Officer, also participates in all the meetings of the Control Risks and Sustainability Committee, ensuring alignment between operational implementation and strategic oversight with the support of the relevant departments.

In addition, the Executive Director and Chief Corporate & Supply Officer coordinates the Cyber Security Steering Committee, established in 2022, which plays a key role in supporting the Group in the management and monitoring of cybersecurity improvement initiatives.

The Cyber Security Steering Committee is composed of: the Group Chief Corporate & Supply Officer; Stone Island's Chief Corporate & Operating Officer; the Group Chief Information & Technology Transformation Officer; the Group Chief Information Security Officer (CISO); the Group Internal Audit Director; the Group Senior Risk Manager; and the HR Business Partner responsible for the IT department's organisational structure.

As a final point, the IT department is responsible for defining the strategic direction and implementing technological solutions that enhance business operations and support innovation. Within this department, the CISO plays a central role in safeguarding the Group's information and technology assets. The CISO leads the development and execution of robust cybersecurity strategies, ensures, with the help of the relevant departments, compliance with regulatory requirements, manages and mitigates risks, and defines contingency plans to respond to potential security incidents or emergencies. To further strengthen its commitment to safeguarding information and technology assets, the Group has also adopted a dedicated Information Security Policy.

As a result of all combined efforts, no significant security breaches were recorded in 2024, reinforcing the effectiveness of the governance framework and security controls in place.

Policy

The **Information Security Policy** defines the key principles and guidelines that serve as the basis for the Group's approach to cybersecurity and data protection. Among its core objectives, the Policy promotes the continuous improvement of information security systems, the safeguarding of data integrity and the proactive monitoring and management of potential threats. It also clearly outlines

the roles and responsibilities of individuals across the organisation with respect to information security.

The main roles and responsibilities include the following:

- Application Competence Center (ACC): ensures secure software development and supports cybersecurity initiatives.
- Cybersecurity Department: oversees the Group's overall information security strategy, updates security plans, delivers training, manages cybersecurity requirements in contracts and projects and handles incident response.
- Networking Department: manages and secures the Group's network infrastructure.
- IT Business Partner: represents the IT department in business projects and supports cybersecurity-related activities.
- Technology Competence Center (TCC): maintains the Group's technology infrastructure, manages system updates and ensures effective disaster recovery procedures.

In addition, the Policy sets specific requirements to be met by third parties, including suppliers, to ensure a consistent and robust security posture across the entire value chain. These requirements cover the following areas:

1. **Access Control**: ensuring that only authorized users have access to certain data and systems.
2. **Data Encryption**: protecting data both in transit and at rest using encryption techniques.
3. **Authentication and Authorization**: verifying the identity of users and ensuring they have the necessary permissions to access resources.
4. **Network Security**: protecting the integrity and usability of network and data, including firewalls, intrusion detection systems, and secure communication protocols.
5. **Incident Response**: establishing clear procedures and policies for responding to security breaches or incidents.
6. **Compliance and Legal Requirements**: ensuring adherence to applicable legal and regulatory frameworks.
7. **Physical Security**: protecting physical assets and facilities from unauthorized access or damage.
8. **Risk Management**: identifying, assessing and mitigating security risks.
9. **Security Training and Awareness**: Fostering a culture of security through staff training and ongoing awareness initiatives.

Management program

In line with the principles set out in the Information Security Policy, the Group has launched a comprehensive Information Security Management Program aimed at turning these commitments into structured and measurable actions. Key elements of this program include the development and regular testing of Business Continuity and Disaster Recovery plans, specifically designed to address the potential impacts of cyber threats on critical business operations.

As part of its proactive approach, the Group conducts periodic vulnerability assessments across its infrastructure - including endpoints, servers and cloud environments - with findings reviewed and prioritized for remediation by internal IT and security teams. To ensure objectivity and compliance, independent security audits are also commissioned annually, in addition to the ongoing internal control activities.

The Group collaborates with several external IT service providers, many of whom deliver services via cloud-based platforms certified to international standards such as ISO/IEC 27001, SOC 2 and CSA STAR. These partnerships are governed by formalized vendor risk assessments and continuous monitoring of compliance obligations.

To further strengthen operational resilience, the Group has implemented a formal incident escalation and reporting procedure that enables all employees to promptly report suspected incidents, vulnerabilities or anomalous behaviors. This procedure is embedded within the corporate intranet and supported by clear guidelines and automated alerting mechanisms.

Complementing these measures, the Group conducts regular awareness and training programs tailored to different roles and responsibilities—ranging from basic security hygiene for general staff to targeted workshops for IT administrators and executives. Between 2024 and the first half of 2025, some simulation campaigns (such as phishing tests) were carried out to evaluate readiness and responsiveness.