

An aerial view of a city skyline, featuring several prominent skyscrapers and a body of water in the foreground. A large, rounded blue overlay is positioned in the center of the image, containing white text. The text includes the title 'SCOR Information Security Policy' and the subtitle 'Public Version January 2026'. The background shows a mix of modern glass skyscrapers and older brick buildings, with a clear blue sky and scattered white clouds.

IT Security

# SCOR Information Security Policy

Public Version January 2026

# SCOR Information Security Policy

## Document Information

SCOR Information Security policies set minimum standards and controls across all entities and may be strengthened to meet local legal and regulatory requirements.

They apply to all SCOR entities, employees, contractors, and Third Parties that handle SCOR data.

The policies are reviewed annually to ensure alignment with evolving regulations and best practices.

## Objectives

Information Security management policies aim to ensure that SCOR Data, Applications and Systems get the required level of Confidentiality, Integrity, and Availability and Safety (CIAS) needed to conduct SCOR operations and business, and thus ensure that:

- Data remains accurate, consistent, and protected against unauthorized access or modification throughout its lifecycle.
- Active monitoring and incident response mechanisms are established to continuously track cybersecurity threats, responding promptly to incidents, and communicating transparently with stakeholders.
- Information security controls are regularly reviewed and updated to address evolving Risks.
- Security responsibilities are defined and shared across the entire workforce.
- External partners and suppliers comply with established security standards to protect SCOR Data, Applications and Systems.

## Core Principles

Our comprehensive Information Security policies are designed to prevent system compromises, fraudulent transactions, Data breaches, and Service disruptions, and are built on four core principles:

- **Confidentiality:** ensure that confidential Information and Personal Data are accessible only to authorized individuals and protected from unauthorized disclosure.
- **Integrity:** maintain the accuracy, consistency, and trustworthiness of Data throughout its lifecycle.
- **Availability:** guarantee that Information and Systems are accessible to authorized users when needed, minimizing downtime and disruptions.
- **Safety:** protect Data and Systems from harm, ensuring resilience against threats and reducing associated with technology failures, breaches, or malicious actions.

Both SCOR personnel and Third Parties must comply with the Cybersecurity, Data protection, and operational resilience requirements set in SCOR's Policies.

## Business Continuity & operational Resilience

Business Continuity Plan and Disaster Recovery Plan (BCP/DRP) are established and regularly tested to ensure effective continuity of operations in the event of significant disruptions.

To strengthen resilience, SCOR conducts a comprehensive operational resilience testing program built on three pillars:

- Assessment: regular audits, risk evaluations, vulnerability scans, and Red Team exercises.
- Testing: disaster recovery drills, backup restoration, penetration tests, and BCP simulations.
- Monitoring tools: centralized platform to track audit findings, recommendations, and remediation progress.

## Vulnerability and Patch Management

SCOR operates a comprehensive, risk-based vulnerability and patch management program across all platforms and environments, proactively identifying and remediating weaknesses to strengthen defenses against evolving cyber threats. This includes:

- Prioritization using *Common Vulnerability Scoring System* (CVSS) scoring from the US *National Vulnerability Database* (NVD).
- Remediation planning informed by assessments and continuous monitoring, time-to-remediate benchmarks, and automated tracking.
- Secure flaw remediation integrated into configuration management, with automated updates where appropriate and removal of outdated components.
- Regular vulnerability scanning, content updates for new *Common Vulnerabilities and Exposures* (CVEs), and management of publicly discoverable information to reduce exposure.
- Independent penetration testing and Red Team exercises.

## Threat Management

SCOR adopts industry-recognized Threat management practices to strengthen its Information Technology against Cyber and physical Threats. The approach focuses on actionable intelligence and proactive Defense, enabling SCOR to anticipate Risks and implement effective countermeasures:

- A Threat Awareness program (“Cyber Watch”) for bilateral/multilateral information sharing.
- Integration of Threat intelligence feeds (e.g., CERT alerts) to stay current on vulnerabilities and exploits.
- Threat hunting to proactively search for sophisticated Threats beyond traditional Defenses.
- A structured and centralized Threat Catalog to guide teams on Risk assessment and support consistent identification, prioritization, and mitigation of known Threats.

## Continuous Monitoring and 24/7 Security Operations

SCOR maintains enterprise-wide situational awareness via centralized log collection and analysis, real-time alerting, and layered detection capabilities through the following mechanisms:

- Event logging, automated log review, and secure log retention (separate repositories, integrity protection, and lifecycle controls).
- Network *Intrusion Detection and Prevention Systems* (IDS/IPS) at the perimeter and critical segments.
- Monitoring of Inbound/Outbound traffic and *Wireless Intrusion Detection System* (WIDS).
- Host-based monitoring for servers, workstations, and mobile devices, and *File Integrity Monitoring* (FIM).
- Automated correlation of telemetry from monitoring tools to accelerate detection and response.

To reinforce this capability, our *Security Operations Center* (SOC) operates 24/7 to detect and respond to malicious activities. All events are correlated in real time against predefined Cyber Risks scenarios, ensuring rapid identification of Threats.

## Incident Response and Cyber resilience

SCOR operates a sound Incident Management capability to detect, analyze, contain, and recover from Cybersecurity and Data privacy incidents. This program strengthens SCOR's ability to respond effectively to incidents, minimizing impact and accelerating recovery and includes:

- A maintained and annually reviewed Incident Response Plan (IRP) with tabletop simulations and scenario testing.
- Insider Threat handling, red-flag identification, and dynamic containment options (e.g., isolation, controlled service reduction through graceful degradation) based on incident criticality.
- Cooperation with regulators, law enforcement, and supply-chain partners when appropriate.
- Data breach notifications and communication processes, including Crisis communications practices to support transparency and protect stakeholders' trust.
- Root cause analysis and lessons learned to drive continuous improvement.

## Security Awareness and Training

All employees are responsible for complying with security requirements and reporting anomalies. SCOR fosters a security-conscious culture that equips employees and partners to make informed decisions:

- Mandatory awareness programs instill foundational practices such as secure handling of data, safe use of collaboration tools, strong authentication, and reporting of anomalies.

- Role-based trainings offer deeper capability for engineers, developers, administrators, and business owners, tailored to the risks inherent in their duties.
- Phishing simulations and just-in-time education strengthen resilience against social engineering and reinforce learning with immediate feedback.
- Clear guidance on acceptable use and data protection, aligned with our values, makes accountability visible and practical.

## Third Party Security Management

SCOR enforces strict security requirements for Third Parties, whether they are vendors, service providers, independent contractors and partners, who access SCOR Systems or Data:

- Third parties are subject to security due diligence, contractual obligations, and ongoing oversight under our procurement and assurance frameworks.
- Additional security requirements apply for Third Parties delivering critical Services or Applications.

By applying stringent security controls, contractual safeguards, and continuous monitoring of third-party engagements, SCOR minimizes external risks and protects its Systems and Data.

## Internal controls & Compliance

SCOR ensures effective governance and compliance through its Internal Control System (ICS) framework. This framework connects business processes to associated Risks and defines the IT controls needed to mitigate them, ensuring full alignment with international regulations and standards:

- Internal control responsibilities are clearly structured in three Lines of Defense (LoD):
  - First LoD: operational teams apply processes and execute controls.
  - Second LoD: Risk Management reviews control effectiveness.
  - Third LoD: the Group Internal Audit (GIA) provides independent assurance through regular testing.
- Regulatory changes are continuously monitored and incorporated into updates, reinforcing SCOR commitment to transparency and resilience.
- Security controls are monitored and reported through annual resilience reports, quarterly dashboards, and IT performance reviews.

## Reporting and escalation process

All Users of Information Systems and Services must promptly report any observed or suspected security incidents, vulnerabilities, data breaches, or suspicious activities to the local IT support or the CISO office so they can liaise with the Regional Compliance Officer on any reporting obligation to authorities.

## Support & Help

For assistance or inquiries regarding this policy, please contact our [CISO Office](#).



Certified with **wiztrust**

All content published by the SCOR group since January 1, 2024, is certified with Wiztrust. You can check the authenticity of this content at [wiztrust.com](https://www.wiztrust.com).