

IT Security

Politique de Sécurité de l'Information SCOR

Version publique janvier 2026

SCOR
The Art & Science of Risk

Politique de Sécurité de l'Information

Informations générales

Les politiques de Sécurité de l'Information de SCOR définissent des exigences et contrôles minimaux applicables à toutes les entités du Groupe et peuvent être renforcées afin de répondre aux obligations légales ou réglementaires locales.

Elles s'appliquent à l'ensemble des entités et des collaborateurs de SCOR, ainsi qu'aux prestataires et Tiers ayant accès aux données ou aux systèmes de SCOR.

Les politiques sont révisées annuellement afin de garantir leur alignement avec les évolutions réglementaires et les meilleures pratiques internationales.

Objectifs

Les politiques de gestion de la Sécurité de l'Information ont pour objectif de garantir que les Données, Applications et Systèmes SCOR bénéficient du niveau requis de Confidentialité, Intégrité, Disponibilité et Sécurité (CIAS) pour soutenir les opérations et l'activité du Groupe.

Elles visent notamment à assurer que :

- Les données restent exactes, cohérentes et protégées contre tout accès ou modification non autorisés, tout au long de leur cycle de vie.
- Les mécanismes de surveillance active et de réponse aux incidents permettent de suivre les menaces Cyber, de réagir rapidement et d'informer de manière transparente les parties prenantes.
- Les contrôles de sécurité sont régulièrement revus et mis à jour pour répondre à l'évolution des Risques.
- Les rôles et responsabilités en matière de sécurité sont clairement définies et partagées avec l'ensemble du personnel.
- Les partenaires et fournisseurs externes respectent des standards de sécurité adaptés pour protéger les Données, Applications et Systèmes SCOR.

Principes directeurs

Nos politiques exhaustives en matière de Sécurité de l'Information visent à prévenir les compromissions de systèmes, les transactions frauduleuses, les violations de données et les interruptions de services. Elles reposent sur quatre principes fondamentaux :

- Confidentialité : garantir que les Informations confidentielles et les Données Personnelles ne sont accessibles qu'aux personnes autorisées et protégées contre toute divulgation non autorisée.
- Intégrité : maintenir l'exactitude, la cohérence et la fiabilité des Données durant tout leur cycle de vie.

- Disponibilité : garantir que les Informations et les Systèmes sont accessibles aux utilisateurs autorisés en cas de besoin, en minimisant les interruptions et indisponibilités.
- Sécurité : protéger les Données et Systèmes contre les dommages, en renforçant leur résilience face aux menaces et en réduisant les risques liés aux défaillances technologiques, aux brèches ou aux actions malveillantes.

Les collaborateurs SCOR comme les Tiers doivent respecter les exigences en matière de cybersécurité, de protection des données et de résilience opérationnelle définies dans les Politiques SCOR.

Continuité d'activité et résilience opérationnelle

Le Plan de Continuité d'Activité (*Business Continuity Plan*, BCP) et le Plan de Reprise d'Activité (*Disaster Recovery Plan*, DRP) sont établis et régulièrement testés pour garantir la continuité des opérations en cas de perturbation majeure.

Pour renforcer cette résilience, SCOR met en œuvre un programme complet de tests de résilience, fondé sur trois piliers :

- Évaluation : audits réguliers, analyses de risques, scans de vulnérabilité, exercices de type *Red Team*.
- Tests : exercices de reprise après sinistre, restauration de sauvegardes, tests de pénétration, simulations BCP.
- Outils de suivi : plateforme centralisée regroupant les constats d'audit, les recommandations et les plans de remédiation.

Gestion des vulnérabilités et des correctifs

SCOR met en œuvre un programme complet et fondé sur les risques pour la gestion des vulnérabilités et des correctifs, couvrant l'ensemble des plateformes et environnements. Ce programme permet d'identifier et de corriger de manière proactive les faiblesses afin de renforcer les défenses contre les menaces cyber en constante évolution. Il comprend notamment :

- La priorisation basée sur le système de notation CVSS (*Common Vulnerability Scoring System*) de la base de données américaine *National Vulnerability Database* (NVD).
- La planification des remédiations, étayée par l'évaluation et la surveillance continue, les référentiels de délais de remédiation, ainsi que le suivi automatisé de celles-ci.
- L'intégration de la remédiation sécurisée des failles dans la gestion des configurations, avec l'application automatisée des mises à jour lorsque cela est pertinent, et le retrait des composants obsolètes.
- Des analyses de vulnérabilités régulières, l'actualisation des contenus pour intégrer les nouvelles CVEs (*Common Vulnerabilities and Exposures*), ainsi que la gestion des informations publiquement accessibles afin de réduire l'exposition.
- Des tests d'intrusion indépendants et des exercices de type *Red Team*.

Gestion des menaces

SCOR adopte des pratiques de gestion des menaces reconnues dans l'industrie afin de renforcer ses Technologies de l'Information face aux menaces cyber et physiques. Cette approche met l'accent sur une veille exploitable et une défense proactive, permettant à SCOR d'anticiper les risques et de mettre en œuvre des contre-mesures efficaces :

- Un programme de sensibilisation aux menaces (« Cyber Watch ») favorisant le partage bilatéral ou multilatéral d'informations.
- L'intégration de flux de renseignement sur les menaces (par ex. : alertes CERT) afin de rester informé des vulnérabilités émergentes et de leur possible exploitation.
- Des activités de *Threat Hunting* pour rechercher de manière proactive des menaces sophistiquées contournant les défenses traditionnelles.
- Un catalogue des menaces structuré et centralisé pour guider les équipes dans l'évaluation des risques et soutenir de façon cohérente l'identification, la priorisation et la mitigation des menaces connues.

Surveillance continue et SOC 24/7

SCOR assure une surveillance en continu grâce à une collecte et analyse centralisées des journaux, des alertes en temps réel et des capacités de détection multicouches mises en œuvre au travers des mécanismes suivants :

- Journalisation des événements, revue automatisée et conservation sécurisée des journaux (référentiels séparés, protection de l'intégrité et contrôles du cycle de vie).
- Systèmes de détection et de prévention d'intrusion réseau (*Intrusion Detection and Prevention Systems*, IDS/IPS) au niveau du périmètre et des segments critiques.
- Surveillance des flux entrants/sortants et détection des intrusions sur les réseaux sans fil (*Wireless Intrusion Detection System*, WIDS).
- Surveillance des hôtes (serveurs, postes, mobiles), et des fichiers critiques (*File Integrity Monitoring,* FIM).
- Corrélation automatisée des données de télémétrie provenant des outils de surveillance afin d'accélérer la détection et la réponse.

Pour renforcer cette capacité, notre *Security Operations Center* (SOC) fonctionne 24h/24 et 7j/7 afin de détecter et de répondre aux activités malveillantes. Tous les événements sont corrélés en temps réel avec des scénarios de risques Cyber prédéfinis, garantissant une identification rapide des menaces.

Gestion des incidents et Cyber-résilience

SCOR dispose de processus robustes de gestion des incidents, visant à détecter, analyser, contenir et résoudre les incidents de Cybersécurité ou de protection des données. Ce dispositif renforce l'aptitude de SCOR à réagir efficacement aux incidents, en minimisant leur impact et en accélérant la reprise. Il comprend notamment :

- Un plan de réponse aux incidents (*Incident Response Plan*, IRP) maintenu à jour et testé annuellement par des exercices de simulation.

- La gestion des menaces internes, l'identification des signaux d'alerte (*Red flags*) et des options de confinement dynamique (par ex. : l'isolation, ou la réduction contrôlée des services par dégradation progressive) en fonction de la criticité de l'incident.
- La coopération avec les régulateurs, les autorités et les partenaires externes, lorsque cela est nécessaire.
- Les procédures de notification en cas de violation de données et les processus de communication associés, incluant les pratiques de communication de crise pour garantir la transparence et préserver la confiance des parties prenantes.
- L'analyse de causes (*Root Cause Analysis*) et le retour d'expérience visant l'amélioration continue.

Sensibilisation et formation à la sécurité

Tous les collaborateurs sont tenus de respecter les exigences de sécurité et de signaler toute anomalie. SCOR encourage une culture de la sécurité qui permet aux employés et aux partenaires de prendre des décisions éclairées :

- Des programmes de sensibilisation obligatoires assurent l'acquisition des principes fondamentaux, notamment la gestion sécurisée des données, l'utilisation maîtrisée des outils collaboratifs, l'authentification forte et le signalement des anomalies.
- Des formations différenciées en fonction des rôles renforcent les compétences des populations exposées à des risques particuliers (ingénieurs, développeurs, administrateurs, responsables métiers), conformément aux exigences liées à leurs responsabilités opérationnelles.
- Des simulations d'hameçonnage et des modules de formation contextualisés (*just-in-time*) renforcent la capacité des collaborateurs à résister aux techniques d'ingénierie sociale et consolident l'apprentissage grâce à un retour d'information immédiat.
- Des lignes directrices claires relatives à l'usage acceptable des ressources et à la protection des données, alignées avec nos valeurs, favorisent l'appropriation des responsabilités et contribuent à une application cohérente des contrôles au sein du Groupe.

Gestion de la sécurité des Tiers

SCOR impose des exigences de sécurité strictes à l'ensemble de ses Tiers, qu'il s'agisse de fournisseurs, de prestataires, d'entrepreneurs indépendants ou de partenaires, dès lors qu'ils accèdent aux Systèmes ou aux Données du Groupe :

- Les Tiers sont soumis à une évaluation de sécurité préalable (*Due Diligence*), à des obligations contractuelles formalisées et à un suivi continu, conformément à nos dispositifs de gestion des achats et d'assurance.
- Des exigences de sécurité renforcées s'appliquent aux Tiers fournissant des services ou applications critiques.

En combinant contrôles de sécurité rigoureux, garanties contractuelles adaptées et surveillance continue des engagements Tiers, SCOR minimise les risques externes et assure la protection de ses Systèmes et de ses Données.

Contrôles internes et conformité

SCOR assure une gouvernance efficace et une conformité renforcée grâce à son cadre de Contrôle Interne (*Internal Control System*, ICS). Ce cadre articule les processus métiers avec les risques associés, et définit les contrôles informatiques nécessaires pour les atténuer, garantissant ainsi une conformité avec les réglementations et standards internationaux :

- Les responsabilités en matière de contrôle interne sont organisées selon le modèle des Trois Lignes de Défense (*Line of Defense*, LoD) :
  - 1ère LoD : les équipes opérationnelles appliquent les processus et exécutent les contrôles.
  - 2ème LoD : la gestion des risques supervise la conception des contrôles, en assure la gestion et évalue leur performance.
  - 3ème LoD : l'Audit Interne Groupe (GIA) fournit une assurance indépendante au travers de revues et de tests réguliers.
- Les évolutions réglementaires font l'objet d'une veille continue et sont intégrées aux mises à jour du dispositif, réaffirmant l'engagement de SCOR en matière de transparence, de conformité et de résilience.
- Les contrôles de sécurité sont suivis et reportés dans le cadre de rapports annuels de résilience, de tableaux de bord trimestriels et de revues de performance IT.

Procédure de reporting et d'escalade

Tous les Utilisateurs des Systèmes et Services Informatiques doivent signaler sans délai tout incident de sécurité observé ou suspecté, toute vulnérabilité, violation de données ou activité inhabituelle. Ces signalements doivent être adressés au support IT local ou au bureau du CISO, afin de permettre la coordination avec le Responsable de Conformité régional concernant les obligations de notification éventuelles auprès des autorités compétentes.

Support & Assistance

Pour toute question relative à cette politique, contactez le Bureau du CISO.

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.