					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P30					Titre du document : **Politique de réponse aux incidents**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clause 8.1, Clause 9	Processus structurés de gestion des risques et de réponse aux incidents
ISO/IEC 27002:2022	Contrôles 5.25–5.27	Rôles, signalement, réponse et amélioration en matière d'incidents
NIST SP 800-53 Rev.5	IR-1 à IR-9	Cycle de vie complet de la réponse aux incidents
RGPD de l'UE	Article 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Délais de notification des violations, obligations de signalement et communication aux personnes concernées
NIS2 de l'UE	Article 23(1)–(4)	Notification à l'autorité nationale et signalement structuré
DORA de l'UE	Article 17(1)–(3)	Signalement des incidents majeurs liés aux TIC pour les entités financières
COBIT 2019	DSS02, DSS04, MEA	Définit, surveille et évalue la gestion des incidents, la continuité et l'évaluation

1. Objet

1.1 La présente politique établit un cadre formel pour l'identification, le signalement, l'analyse, le confinement, la réponse, le rétablissement et l'évaluation post-incident des incidents de sécurité de l'information affectant l'organisation.

1.2 Elle impose des réponses rapides, coordonnées et efficaces afin de réduire au minimum les perturbations opérationnelles, les pertes financières, les atteintes à la réputation et les risques de non-conformité réglementaire.

1.3 La politique favorise également l'amélioration continue du niveau de cyberrésilience de l'organisation grâce aux enseignements tirés et à l'intégration des constats post-incident dans la gouvernance, les outils et les programmes de formation.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 L'ensemble du personnel, y compris les employés, sous-traitants, consultants et prestataires de services tiers

2.1.2 Tous les systèmes d'information, applications, infrastructures, réseaux et données, qu'ils soient sur site, dans le cloud ou hybrides

2.1.3 Tous les types d'incidents de sécurité, y compris, sans s'y limiter :

2.1.3.1 Accès non autorisé ou élévation de privilèges

2.1.3.2 Attaques par logiciels malveillants et rançongiciels

2.1.3.3 Attaques par déni de service (DoS/DDoS)

2.1.3.4 Perte, fuite ou exfiltration de données

2.1.3.5 Usage abusif interne ou manquements à la politique

2.1.3.6 Atteintes à la sécurité physique affectant les actifs numériques

2.2 La politique couvre la détection, le triage, l'investigation, l'escalade, le confinement, le traitement des éléments de preuve, la notification, le rétablissement et l'analyse des causes racines.

3. Objectifs

3.1 Établir une capacité de réponse aux incidents reproductible et évolutive permettant la détection, la classification et l'atténuation rapides des incidents de sécurité.

3.2 Réduire au minimum l'impact métier des événements de sécurité au moyen de procédures structurées de confinement, d'éradication et de rétablissement des systèmes.

3.3 Garantir que le signalement et la réponse aux incidents sont conformes aux exigences légales, réglementaires et contractuelles, en particulier celles relatives aux délais de notification des violations et au traitement des éléments de preuve.

3.4 Soutenir la transparence et la responsabilisation au moyen d'une journalisation, d'une documentation et d'un suivi des indicateurs appropriés pour tous les incidents de sécurité.

3.5 Favoriser l'amélioration continue au moyen des revues post-incident, des actions correctives et de la formation des parties prenantes.

4. Rôles et responsabilités

4.1 Responsable de la sécurité des systèmes d'information (RSSI)

4.1.1 Est responsable du dispositif de réponse aux incidents, veille à l'application de la politique et supervise la coordination des incidents à l'échelle de l'organisation.

4.1.2 Agit en tant qu'interlocuteur principal auprès des autorités de régulation, de la direction générale et du conseil juridique externe lors d'incidents majeurs.

4.2 Coordinateur de la réponse aux incidents

4.2.1 Coordonne les équipes de réponse pluridisciplinaires, gère les flux de traitement et suit l'état du confinement et du rétablissement.

4.2.2 Déclenche et conduit les revues post-incident et veille à ce que les actions correctives soient consignées et mises en œuvre.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exigences de revue et de mise à jour

9.1 La présente politique doit être revue au moins une fois par an et mise à jour si nécessaire afin d'intégrer :

9.1.1 Les évolutions du paysage des menaces, des types d'incidents ou des vecteurs d'attaque

9.1.2 Les enseignements tirés des incidents majeurs, des quasi-accidents ou des constats réglementaires

9.1.3 Les mises à jour des lois et réglementations applicables (par exemple, RGPD, DORA, NIS2)

9.1.4 Les retours d'information issus des exercices de réponse aux incidents et des revues post-incident

9.2 Le RSSI est responsable de l'initiation et de la coordination du processus de revue, en concertation avec :

9.2.1.1 Le conseil juridique et le DPD

9.2.1.2 Le SOC et les opérations informatiques

9.2.1.3 Les équipes de continuité d'activité et de gestion des risques

9.2.1.4 La direction générale

9.3 Les modifications de la politique doivent être :

9.3.1 Documentées dans un référentiel soumis à gestion des versions

9.3.2 Communiquées à toutes les équipes concernées et intégrées à la formation de sensibilisation

9.3.3 Validées au moyen d'exercices de réponse aux incidents sur table ou en conditions réelles dans les trois mois suivant leur approbation

9.4 Les mises à jour urgentes déclenchées par des menaces émergentes, des constats d'audit ou de nouvelles obligations légales doivent être mises en application immédiatement et consignées dans l'historique des révisions de la politique.

10. Politiques associées et articulations

10.1 La présente politique est appuyée par les politiques organisationnelles suivantes et articulée avec elles :

10.1.1 P1 – Politique de sécurité de l'information : établit l'exigence générale d'opérations fondées sur les risques et préparées à la gestion des incidents.

10.1.2 P5 – Politique de gestion des changements : garantit que les activités de confinement et de rétablissement impliquant l'infrastructure ou les services suivent des procédures formelles.

10.1.3 P13 – Politique de classification et d'étiquetage des données : soutient la classification de la gravité des incidents en fonction de la sensibilité des données.

10.1.4 P15 – Politique de sauvegarde et de restauration : permet le rétablissement après un rançongiciel ou des attaques destructrices avec garantie d'intégrité.

10.1.5 P18 – Politique relative aux contrôles cryptographiques : définit les mesures de chiffrement qui réduisent l'impact des incidents et les risques d'exposition des données.

10.1.6 P22 – Politique de journalisation et de surveillance : fournit la visibilité sur les événements, les mécanismes d'alerte et la conservation des journaux nécessaires à une détection efficace et à l'analyse forensique.

10.1.7 P29 – Politique relative aux données de test et aux environnements de test : garantit que les incidents affectant les systèmes hors production sont également traités de manière structurée et sécurisée.

10.1.8 P33 – Politique d'audit et de surveillance de la conformité : valide la préparation aux incidents et l'efficacité de la réponse au moyen d'audits structurés et d'évaluations de conformité.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001: Clause 8.1 – Planification et maîtrise opérationnelles : processus structurés pour gérer les risques et planifier la réponse aux incidents.

11.2 ISO/IEC 27002:2022 – Contrôles 5.25–5.27 : responsabilités relatives à la gestion des incidents, au signalement, à la réponse, à la communication et à l'amélioration.

11.3 NIST SP 800-53 Rev.5 : IR-1 à IR-9, AU-6, PL-2 : exigences complètes relatives au cycle de vie de la réponse aux incidents, à l'audit et à la planification de la sécurité.

11.4 RGPD de l'UE : Articles 33/34 : obligations d'information à l'autorité de contrôle et exigences de notification des personnes concernées (avec exceptions définies).

11.5 Directive NIS2 de l'UE (2022/2555) : Article 23 : signalement national obligatoire, avec obligations de signalement intermédiaire et final.

11.6 DORA de l'UE (2022/2554) : Article 17 : exigences de signalement aux autorités des incidents TIC pour les établissements financiers.

11.7 COBIT 2019 : DSS02, DSS04, MEA01 : gestion des incidents de service et de la continuité, ainsi que surveillance de la performance et de la conformité.