Politique de Gestion de Crise Cyber

1. Objectif

E1: Cette politique vise à définir les procédures et rôles pour la gestion d'une crise cyber afin de minimiser l'impact sur l'entreprise et d'assurer un retour à la normale rapide et sécurisé.

2. Champ d'application

E2: Cette politique s'applique à tous les employés, prestataires et partenaires impliqués dans la gestion des incidents de cybersécurité affectant les systèmes d'information de l'entreprise.

3. Structure de Gestion de Crise

E3: **Comité de gestion de crise** - Composé de la direction, du Responsable Sécurité des Systèmes d'Information (RSSI), des responsables IT et de la communication.
E4: **Cellule technique de réponse** - Dédiée à l'analyse technique et à la mise en œuvre des mesures correctives.
E5: **Cellule communication** - Chargée de la gestion des communications internes et externes.
E6: **Support juridique et conformité** - Assure le respect des obligations réglementaires et coordonne avec les autorités.

4. Phases de Gestion de Crise

E7: **Détection et Qualification** - Identification de l'incident, classification selon son impact et activation du plan de crise.
E8: **Confinement et Remédiation** - Mise en place de mesures pour limiter la propagation de l'incident et mise en œuvre des correctifs.
E9: **Communication de Crise** - Coordination des messages avec les parties prenantes (employés, clients, autorités, médias).
E10: **Retour à la Normale** - Rétablissement des systèmes impactés et vérifications de sécurité.
E11: **Retour d'Expérience** - Analyse post-incident pour améliorer les procédures et prévenir les récurrences.

5. Outils et Moyens

E12: Solutions de détection et réponse aux incidents (SIEM, SOC, EDR).
E13: Procédures de sauvegarde et restauration.
E14: Plans de communication prédéfinis.
E15: Simulations régulières de gestion de crise cyber.

6. Obligations Légales et Réglementaires

E16: Notification des incidents conformément aux obligations (RGPD, NIS2, etc.).

E17: Coordination avec les autorités et agences nationales de cybersécurité.

7. Surveillance et Amélioration Continue

E18: Tests et exercices périodiques pour évaluer la réactivité de l'organisation.

E19: Mise à jour régulière des plans en fonction des menaces émergentes.

Cette politique est révisée annuellement ou après chaque incident majeur.