| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insérez ici la dénomination de l'entité juridique enregistrée | | | | | | | |
| Numéro du document :<br>P32 | | | | | Titre du document :<br>**Politique de continuité d'activité et de reprise après sinistre** | | | | | | | |
| Version :<br>1.0 | | Date d'entrée en vigueur :<br>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 | Article 8 | |
| ISO/IEC 27002:2022 | Mesures 5.29, 5.30 | |
| NIST SP 800-53 Rev.5 | CP-1 à CP-11 | |
| NIST SP 800-34 Rev.1 | Planification de la continuité | Référentiel |
| ISO 22301:2019 | | Exigences relatives au système de management de la continuité d'activité |
| RGPD de l'UE | Article 32 | |
| NIS2 de l'UE | Article 21(2)(f) | |
| DORA de l'UE | Article 10 | |
| COBIT 2019 | DSS | |

**1. Objet**

1.1. La présente politique définit les contrôles obligatoires et les responsabilités visant à garantir la capacité de l'organisation à maintenir ou à rétablir les opérations métier critiques et les systèmes TIC de support pendant et après un incident perturbateur.

1.2. Elle vise à protéger les personnes, la stabilité opérationnelle, les obligations légales, les engagements envers les clients et la réputation de l'organisation en intégrant la résilience au moyen d'une planification proactive et de capacités de reprise validées.

1.3. La présente politique constitue le fondement du dispositif de continuité d'activité et de reprise après sinistre de l'organisation et garantit la conformité aux exigences réglementaires, contractuelles et sectorielles applicables.

**2. Champ d'application**

2.1. La présente politique s'applique à toutes les unités organisationnelles, à tous les systèmes d'information, processus métier, membres du personnel et services tiers classés comme critiques ou essentiels sur la base des résultats de l'analyse d'impact sur l'activité (BIA).

**2.2. La politique couvre :**

2.2.1. Les perturbations d'origine naturelle ou humaine, y compris les cyberattaques, les défaillances d'infrastructure, les indisponibilités de centres de données, les pandémies et les interruptions de services fournisseurs

2.2.2. La planification, les tests et l'amélioration continue des plans de continuité d'activité (PCA) et des plans de reprise après sinistre (DRP)

2.2.3. Les rôles et responsabilités relatifs à la réponse d'urgence, à la coordination de la reprise et à l'escalade des incidents

2.3. L'ensemble du personnel assumant des responsabilités en matière de continuité ou de reprise, y compris les équipes informatiques, les responsables métier, les gestionnaires de crise et les fournisseurs, est soumis aux dispositions de la présente politique.

**3. Objectifs**

3.1. Assurer la continuité des opérations et des services métier au moyen de procédures prédéfinies et testées, afin de réduire au minimum les impacts opérationnels, réputationnels et juridiques.

3.2. Rétablir les systèmes TIC dans les délais définis par les objectifs de temps de reprise (RTO) et les objectifs de point de reprise (RPO), en cohérence avec les niveaux de tolérance au risque métier.

3.3. Attribuer la responsabilité de la planification, de l'exécution et de la gouvernance de la continuité d'activité et de la reprise après sinistre à l'échelle de l'organisation.

3.4. Veiller à ce que les capacités de continuité fassent l'objet de tests réguliers, soient maintenues et améliorées sur la base de scénarios réalistes et des constats d'audit.

3.5. Respecter les obligations de conformité au titre des normes ISO, du NIST, du RGPD, de DORA et de NIS2, en appui au devoir de diligence en matière de résilience opérationnelle et de disponibilité.

**4. Rôles et responsabilités**

**4.1. Haute direction**

4.1.1. Approuve la Politique de continuité d'activité et de reprise après sinistre et en garantit l'alignement stratégique.

4.1.2. Alloue le budget et les ressources nécessaires à la continuité d'activité, à la réponse d'urgence et aux exercices de reprise.

**4.2. Responsable de la continuité d'activité**

4.2.1. Est responsable de l'élaboration et du maintien des PCA à l'échelle de l'organisation, ainsi que de la coordination des tests de continuité.

4.2.2. Tient à jour le calendrier des analyses d'impact sur l'activité (BIA), facilite les formations et veille à ce que la documentation respecte les exigences de conformité.

[ ... 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 faire l'objet d'une revue annuelle par le Responsable de la continuité d'activité et le RSSI afin de garantir son alignement avec :**

9.1.1. Les changements affectant les opérations métier, les systèmes critiques ou l'infrastructure

9.1.2. Les enseignements tirés des incidents, des audits, des exercices sur table ou des tests de reprise après sinistre

9.1.3. Les obligations réglementaires ou contractuelles mises à jour (par exemple : DORA, RGPD, exigences clients en matière de RTO/RPO)

9.1.4. Les évolutions de l'appétence au risque de l'organisation ou de la stratégie de continuité

**9.2. Les revues doivent inclure :**

9.2.1. La validation de la pertinence des plans et des coordonnées de contact

9.2.2. La réévaluation des RTO, des RPO et de la hiérarchisation des niveaux de reprise

9.2.3. L'évaluation de la capacité des services de sauvegarde et de reprise après sinistre

9.2.4. Le retour d'information des parties prenantes ayant exécuté des plans de reprise ou des tests récents

**9.3. Toutes les modifications de la politique doivent être :**

9.3.1. Gérées sous gestion de versions avec justification documentée et validation des parties prenantes

9.3.2. Communiquées au personnel et aux équipes concernés avec les responsabilités mises à jour

9.3.3. Répercutées dans les formations, supports de sensibilisation et procédures opérationnelles mis à jour

9.4. Des mises à jour intermédiaires d'urgence doivent être publiées en cas de changement organisationnel majeur, d'obligation légale ou de constat critique rendant les plans actuels ou la politique inapplicables.

## 10. Politiques associées et articulations

### 10.1. La présente politique s'articule avec les documents clés suivants :

10.1.1. P1 – Politique de sécurité de l'information : établit l'exigence d'opérations résilientes fondées sur les risques dans toutes les situations.

10.1.2. P5 – Politique de gestion des changements : garantit que toute modification d'infrastructure ou de configuration liée à la reprise suit des circuits documentés et approuvés.

10.1.3. P14 – Politique de conservation et d'élimination des données : encadre le cycle de vie des supports de sauvegarde et des données restaurées utilisées dans les opérations de continuité.

10.1.4. P15 – Politique de sauvegarde et de restauration : impose des contrôles relatifs à la fréquence des sauvegardes, à leur sécurité et à la vérification des restaurations.

10.1.5. P18 – Politique relative aux contrôles cryptographiques : garantit que les processus de reprise respectent les exigences de chiffrement et de confidentialité.

10.1.6. P22 – Politique de journalisation et de surveillance : prend en charge la détection et l'escalade des événements ayant un impact sur la continuité.

10.1.7. P30 – Politique de réponse aux incidents : définit les processus de confinement, d'escalade et d'analyse de la cause racine en cohérence avec les déclencheurs de continuité.

10.1.8. P33 – Politique d'audit et de surveillance de la conformité : valide l'intégrité et l'efficacité des pratiques de continuité et de reprise dans l'ensemble des systèmes et des processus.

## 11. Normes et référentiels de référence

11.1. La présente politique est alignée sur des normes internationales reconnues en matière de continuité d'activité et de reprise après sinistre, afin de soutenir l'auditabilité, la résilience et la conformité juridique.

### 11.2. ISO/IEC 27002

11.2.1. Annexe A, Mesure 5.29 – Sécurité de l'information en situation de perturbation : exige le maintien des contrôles de sécurité dans des conditions défavorables.

11.2.2. Annexe A, Mesure 5.30 – Préparation des TIC à la continuité d'activité : impose la préparation, les tests et la validation des capacités de reprise des TIC.

### 11.3. ISO 22301:2019 – Systèmes de management de la continuité d'activité

11.3.1. Fournit le référentiel permettant d'établir, de mettre en œuvre et de maintenir des pratiques de continuité d'activité alignées sur les objectifs de l'organisation et les seuils de risque.

### 11.4. NIST SP 800-34 Rev.1 – Guide de planification de la continuité

11.4.1. Décrit les bonnes pratiques relatives aux plans de continuité des systèmes d'information, y compris l'élaboration de la stratégie de continuité, l'analyse d'impact et les tests des plans.

### 11.5. RGPD de l'UE (2016/679)

11.5.1. Article 32 – Sécurité du traitement : exige la résilience des systèmes et services de traitement ainsi que le rétablissement de la disponibilité des données à caractère personnel et de l'accès à celles-ci dans des délais appropriés après un incident.

### 11.6. Directive NIS2 de l'UE (2022/2555)

11.6.1. Article 21(2)(f) : impose des mesures de continuité d'activité et de gestion de crise pour soutenir la sécurité des réseaux et des systèmes d'information.

**11.7. DORA de l’UE (2022/2554)**

11.7.1. Article 10 – Continuité d’activité des TIC : impose aux entités financières d’élaborer et de tester des plans de continuité des TIC, y compris des RTO/RPO fondés sur les risques et des capacités de basculement.

**11.8. COBIT 2019**

11.8.1. DSS04 – Gérer la continuité : couvre l’ensemble des aspects de la planification de la continuité, y compris l’identification des menaces, l’analyse d’impact, la stratégie de reprise et les tests réguliers.