					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P32S					Titre du document : **Politique de continuité d'activité et de reprise après sinistre**							
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**

Mentions légales (droits d'auteur et restrictions d'utilisation)

(C) 2025 Clarysec LLC. All rights reserved.

Le présent document est la propriété intellectuelle de Clarysec LLC. Aucune partie de ce document ne peut être copiée, réutilisée, distribuée ou modifiée à des fins commerciales ou de mise en œuvre sans autorisation écrite expresse préalable.

Toute utilisation non autorisée est strictement interdite et peut entraîner des poursuites judiciaires.

Pour toute demande de licence, contactez : info@clarysec.com

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Articles 6.1, 6.3, 8	
ISO/IEC 27002:2022	Mesures 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
RGPD	Articles 32, 33	
NIS2	Article 21(2)(f)	
DORA	Article 10	
COBIT 2019	DSS04	

1. Objet

1.1 La présente politique garantit que l'organisation est en mesure de maintenir ses activités et de rétablir les services informatiques essentiels pendant et après des événements perturbateurs tels que des coupures d'électricité, des cyberattaques, des attaques par rançongiciel ou des défaillances système.

1.2 Elle définit un cadre clair de planification de la continuité d'activité et de reprise après sinistre (BC/DR), adapté aux PME ne disposant pas d'équipes informatiques dédiées.

1.3 La présente politique aide l'organisation à satisfaire aux exigences applicables d'ISO/IEC 27001:2022, du RGPD, de NIS2, de DORA et de COBIT 2019, tout en renforçant la résilience opérationnelle et la confiance des clients.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 Tous les systèmes et services critiques pour l'activité (par exemple : messagerie, stockage cloud, plateformes de facturation, dossiers clients)

2.1.2 Tous les employés et prestataires externes de services informatiques responsables de la préparation et de l'exécution du dispositif BC/DR

2.1.3 Tous les types de perturbations, y compris les incidents cyber, les défaillances matérielles, les coupures d'alimentation, les inondations et l'inaccessibilité des bureaux

2.2 Elle couvre :

2.2.1 la gestion des sauvegardes

2.2.2 la planification de la continuité d'activité (BCP)

2.2.3 les opérations de reprise après sinistre

2.2.4 la formation du personnel et les tests

2.2.5 les procédures de réponse juridique et réglementaire

3. Objectifs

3.1 Protéger la capacité de l'organisation à fournir ses services essentiels malgré des perturbations non planifiées.

3.2 Garantir le rétablissement en temps utile des systèmes et des données selon des objectifs de temps de reprise (RTO) prédéfinis.

3.3 Permettre à l’ensemble du personnel d’appliquer les procédures de continuité en situation de crise avec un minimum de confusion.

3.4 Maintenir la conformité réglementaire aux exigences relatives à la protection des données et à la résilience opérationnelle, y compris l’article 32 du RGPD et l’article 21 de NIS2.

3.5 Établir une stratégie de continuité et de reprise pragmatique, testable et adaptée aux PME.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Est responsable du processus BC/DR et de la présente politique

4.1.2 Approuve le plan de continuité d’activité (BCP)

4.1.3 Coordonne la réponse aux incidents et la communication interne pendant les perturbations

4.1.4 Effectue les notifications réglementaires requises (par exemple : notifications de violation de données au titre du RGPD)

4.2 Prestataire informatique / administrateur système

4.2.1 Maintient et teste les sauvegardes

4.2.2 Exécute les procédures de reprise après sinistre lorsqu’elles sont déclenchées

4.2.3 Documente toutes les actions de reprise et tous les événements de restauration système

4.2.4 Signale immédiatement au DG tout incident informatique critique

[... 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 Revue annuelle de la politique et du plan

9.1.1 Le Directeur général (DG) doit veiller à ce que la présente politique et le plan de continuité d’activité (BCP) associé fassent l’objet d’une revue formelle au moins une fois par an.

9.1.2 La revue doit inclure :

9.1.2.1 l’évaluation des risques nouveaux ou émergents

9.1.2.2 la revalidation des RTO/RPO

9.1.2.3 la vérification des informations relatives aux fournisseurs et aux contacts

9.1.2.4 l’alignement avec les changements affectant les systèmes informatiques, les obligations légales ou les opérations

9.2 Mises à jour déclenchées par événement

9.2.1 La présente politique doit également être mise à jour en réponse à :

9.2.1.1 des incidents majeurs ou des perturbations, en particulier si les objectifs n’ont pas été atteints

9.2.1.2 de nouvelles obligations légales ou réglementaires (par exemple : modifications de DORA)

9.2.1.3 des changements touchant les systèmes critiques, les plateformes cloud ou le personnel

9.2.1.4 des constats issus des tests annuels BCP/DR

9.3 Processus de contrôle des changements

9.3.1 Tous les changements doivent être approuvés par le DG

9.3.2 Un historique des versions doit être tenu, incluant la date, la description du changement et son approbateur

9.3.3 La politique mise à jour doit être redistribuée à l'ensemble du personnel concerné, y compris le prestataire informatique et les responsables de département

9.4 Documentation des enseignements tirés

9.4.1 Après les tests ou les perturbations réelles, les enseignements tirés documentés doivent alimenter les futures mises à jour

9.4.2 Ces revues doivent également inclure des évaluations de la performance des fournisseurs et des vérifications de l'adéquation de la réponse

10. Politiques associées et articulations

10.1 La présente politique est étroitement articulée avec les politiques PME suivantes :

10.1.1 P1S – Politique de sécurité de l'information : définit les objectifs de sécurité de haut niveau que les pratiques de continuité et de reprise doivent soutenir.

10.1.2 P4S – Politique de contrôle d'accès : permet la révocation d'urgence ou la restauration des accès utilisateurs en cas de perturbation de l'activité.

10.1.3 P6S – Politique de gestion des risques : constitue le fondement de l'identification, de l'évaluation des risques et de la priorisation des risques liés à la continuité.

10.1.4 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : garantit que les employés sont prêts à agir en cas de perturbation et comprennent le BCP.

10.1.5 P15S – Politique de sauvegarde et de restauration : fournit les procédures techniques spécifiques pour préserver la disponibilité des données et assurer leur récupération.

10.1.6 P17S – Politique de protection des données et de la vie privée : garantit que la planification de la continuité respecte les protections relatives aux données à caractère personnel et se conforme au RGPD pendant et après les incidents.

10.1.7 P22S – Politique de journalisation et de surveillance : prend en charge la détection des événements susceptibles de déclencher les processus BC/DR et fournit une piste d'audit forensique après perturbation.

10.1.8 P30S – Politique de réponse aux incidents : précède directement l'activation du processus de reprise en cas d'incident cyber ou opérationnel.

10.1.9 P31S – Politique de collecte des éléments de preuve et d'investigation forensique : garantit que les éléments de preuve numériques sont collectés dans les scénarios de continuité pour répondre aux besoins de conformité, d'assurance ou d'investigation.

10.2 Ces politiques constituent un cadre cohérent, compatible avec les exigences d'audit, pour la résilience, la responsabilité et la continuité des contrôles dans l'ensemble des opérations de la PME.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001:

11.1.1 Article 6.1 – Exige une planification et un traitement des risques fondés sur les risques, y compris la continuité d'activité et la reprise.

11.1.2 Article 6.3 – Met l'accent sur l'amélioration continue à la suite de perturbations.

11.1.3 Article 8.1 – Implique des contrôles opérationnels, y compris des mesures de continuité documentées.

11.2 ISO/IEC 27002:

11.2.1 Mesure 5.29 – Exige l'établissement et le maintien de dispositions de continuité d'activité.

11.2.2 Mesure 5.30 – Exige le test et la revue de ces dispositions.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – Définit les exigences de planification de continuité.

11.3.2 CP-4 – Implique une formation à la continuité pour le personnel de l'organisation.

11.3.3 CP-6 – Couvre les exigences relatives à un site de stockage alternatif.

11.3.4 CP-7 – Encadre les attentes relatives à un site de traitement alternatif.

11.4 RGPD:

11.4.1 Article 32 – Exige des mesures garantissant la disponibilité continue et la résilience des systèmes et services de traitement.

11.4.2 Article 33 – Déclenche des obligations de notification de violation dans les cas où une défaillance de continuité entraîne une compromission de données à caractère personnel.

11.5 Directive NIS2 (UE) 2022/2555:

11.5.1 Article 21(2)(f) – Exige des capacités de planification de la continuité et de gestion de crise comme condition de préparation au risque cyber.

11.6 Règlement DORA (UE) 2022/2554:

11.6.1 Article 10 – Exige la mise en œuvre de tests de résilience opérationnelle numérique et de capacités de reprise, en particulier pour les PME du secteur financier.

11.7 COBIT 2019:

11.7.1 DSS04 – Gérer la continuité : fournit des orientations de gouvernance d'entreprise pour maintenir et valider la résilience opérationnelle, y compris la responsabilité, les tests, l'intégration des fournisseurs et les revues post-événement.