DOCUMENT 02

Plan de sauvegarde et de reprise d'activité

Protéger vos données et savoir exactement comment repartir après un sinistre, une panne ou un rançongiciel.

Entreprise _____ **Date** _____ **Version** _____

1. Pourquoi ce plan

Une sauvegarde qui n'a jamais été restaurée n'est qu'une hypothèse. Ce plan formalise **ce que vous sauvegardez, où, à quelle fréquence, qui en est responsable** et comment vous restaurez. Il est la réponse la plus efficace à un rançongiciel : si vous pouvez restaurer, vous n'avez aucune raison de payer.

2. Définir vos objectifs : RPO et RTO

- **RPO** (Recovery Point Objective) : quantité maximale de données que vous acceptez de perdre. Ex. : RPO 24 h = vous acceptez de perdre au plus une journée de travail.
- **RTO** (Recovery Time Objective) : durée maximale d'interruption acceptable. Ex. : RTO 8 h = l'activité doit avoir repris dans la journée.

Conseil de l'expert
Posez-vous la question concrète : « Si tout s'arrête ce matin, combien de jours de facturation ou de production puis-je perdre avant que l'entreprise soit en danger ? » C'est votre RTO réel. Il détermine le budget et la solution, pas l'inverse.

3. Inventaire des données et systèmes critiques

Système / donnée	Criticité	Hébergement	RPO cible	RTO cible	Propriétaire / responsable
Messagerie (ex. Microsoft 365)	Vitale	Cloud			
Fichiers partagés (serveur/NAS)	Vitale	Local			
Logiciel de comptabilité / gestion	Élevée	Cloud / local			
Logiciel métier (ERP, CRM)	Élevée	[ ]			

Les quatre premières lignes sont des exemples : adaptez, complétez ou remplacez les lignes. N'oubliez pas : postes nomades, smartphones, comptes cloud (SaaS), site web, caméras/téléphonie.

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

4. La règle 3-2-1 (et ses évolutions)

Principe	Ce que cela signifie concrètement
3 copies	L'original + deux sauvegardes distinctes.
2 supports	Deux types de supports différents (ex. NAS + cloud) pour ne pas tout perdre sur une même panne.
1 copie hors site	Une copie dans un autre lieu ou un cloud (incendie, vol, dégât des eaux).
1 copie hors ligne ou immuable	Une copie déconnectée ou protégée contre l'effacement : c'est elle qui vous sauve d'un rançongiciel, qui chiffre aussi les sauvegardes accessibles.
0 erreur	Restauration testée régulièrement : la sauvegarde est vérifiée, pas supposée.

5. Planification des sauvegardes

Donnée / système	Fréquence	Rétention	Outil / solution	Support / lieu	Responsable

Repères : sauvegarde **quotidienne** pour les fichiers et la messagerie ; **hebdomadaire** en complément (copie complète) ; rétention de **30 jours minimum**, avec une version mensuelle conservée 6 à 12 mois pour revenir avant une infection discrète.

6. Sécuriser les sauvegardes

- **Chiffrer** les sauvegardes (au repos et en transit) et conserver la clé de chiffrement séparément, hors du système sauvegardé.
- Utiliser un **compte dédié** à la sauvegarde, avec authentification multifacteur sur la console d'administration, distinct des comptes d'administration du réseau.
- Prévoir au moins une copie **immuable** ou **déconnectée** (support débranché, stockage objet avec verrouillage de rétention).
- Ne pas laisser de lecteur réseau de sauvegarde monté en permanence sur les postes utilisateurs.
- Surveiller les alertes d'échec de sauvegarde : un responsable est désigné pour les traiter sous 24 h ouvrées.

7. Tests de restauration

Test **au minimum chaque trimestre** : restaurer un fichier, un dossier, puis, une fois par an, un système complet (ou une machine virtuelle) dans un environnement isolé. Consignez chaque test.

Date	Élément restauré	Durée	Résultat	Observations / actions

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

Date	Élément restauré	Durée	Résultat	Observations / actions

8. Procédure de restauration en cas de sinistre

1. **Alerter** le référent et la direction ; activer la fiche réflexe incident (document 05).
2. **Qualifier** : panne, erreur humaine, sinistre physique ou attaque ? En cas d'attaque, **isoler** les machines touchées avant toute restauration.
3. **Vérifier** que la sauvegarde choisie est saine (antérieure à la compromission) et identifier la dernière version utilisable.
4. **Restaurer** d'abord les systèmes vitaux (messagerie, fichiers, facturation), dans l'ordre défini ci-dessus, sur des machines nettoyées ou reconstruites.
5. **Contrôler** l'intégrité des données restaurées avec les utilisateurs clés, puis rouvrir progressivement les accès après changement des mots de passe.
6. **Consigner** la chronologie et en tirer les enseignements (retour d'expérience) sous 15 jours.

9. Rôles et contacts

Rôle	Nom	Coordonnées (tél. / e-mail, hors messagerie de l'entreprise)
Référent sauvegarde		
Suppléant		
Prestataire informatique		
Hébergeur / éditeur de sauvegarde		

Revue annuelle
Ce plan est relu au minimum une fois par an et après tout changement important (nouveau logiciel, déménagement, changement de prestataire). Date de dernière revue : _____ · Prochaine revue : _____

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.