GUIDE PRATIQUE !

DIGITAL FlashUP

GUIDE PRATIQUE

METTRE EN PLACE UNE POLITIQUE DE SAUVEGARDE DE VOS DONNÉES

Un concentré d'idées claires et utiles

Gouvernement Princier
PRINCIPAUTÉ DE MONACO
Extended Monaco Entreprise
MONACO BUSINESS OFFICE

En quelques étapes, définissez quoi sauvegarder, à quelle fréquence, où conserver vos sauvegardes et comment vérifier qu'elles fonctionnent.

Pour vous accompagner, suivons **Azur Services**, une PME fictive de 15 salariés qui utilise une messagerie professionnelle, un logiciel de gestion/facturation, un espace de fichiers partagé et plusieurs applications métiers.

DIGITAL FlashUP

1. Identifiez les données que vous ne pouvez pas vous permettre de perdre

Pesez-vous une question simple :

> **Si nous perdions toutes nos données demain matin, de quoi aurions-nous absolument besoin pour reprendre notre activité ?**

- ☐ Données clients
- ☐ Documents commerciaux et contrats
- ☐ Comptabilité et facturation
- ☐ Données RH
- ☐ Emails et agendas
- ☐ Fichiers et documents de travail
- ☐ Bases de données et logiciels métiers
- ☐ Site Internet et contenus
- ☐ Configurations de vos applications et systèmes
- ☐ Autres : _____

Exemple — Azur Services

L'entreprise identifie comme prioritaires :

1. sa base clients
2. ses devis et factures
3. ses contrats clients
4. ses fichiers de travail partagés
5. sa messagerie

Elle décide en revanche que les anciennes présentations commerciales peuvent attendre quelques jours avant d'être restaurées.

À vous de jouer

Quels sont vos **5 éléments les plus critiques** ?

⚠ **Attention au cloud :** utiliser un service cloud ne signifie pas automatiquement que vous disposez du niveau de sauvegarde dont vous avez besoin. Vérifiez ce que votre fournisseur protège, pendant combien de temps et ce que vous pouvez réellement restaurer.

2. Déterminez combien de données vous pouvez accepter de perdre

Pour chaque donnée importante, demandez-vous :

> **Si je devais restaurer une sauvegarde, quelle quantité de travail pourrais-je accepter de perdre ?**

Exemple — Azur Services

Donnée	Perte maximale acceptable	Sauvegarde décidée
Facturation	1 journée	Quotidienne
Base clients	1 journée	Quotidienne
Fichiers de travail	1 journée	Quotidienne
Documents RH	1 semaine	Hebdomadaire
Archives	1 mois	Mensuelle

Concrètement : si la dernière sauvegarde de la facturation date de vendredi et qu'un incident survient mercredi, Azur Services pourrait perdre plusieurs jours de travail. L'entreprise juge ce risque inacceptable et choisit donc une sauvegarde quotidienne.

À vous de jouer

Mes données / outils	Perte acceptable	Fréquence retenue
_____	☐ 1 h ☐ 1 jour ☐ 1 semaine	_____
_____	☐ 1 h ☐ 1 jour ☐ 1 semaine	_____
_____	☐ 1 h ☐ 1 jour ☐ 1 semaine	_____

3. Organisez vos sauvegardes avec la règle 3-2-1

Retenez simplement :

3 copies

Vos données de travail + **2 copies de sauvegarde**.

2 supports ou environnements distincts

Évitez que toutes vos copies dépendent du même équipement ou du même environnement.

1 copie hors ligne

Conservez au moins une sauvegarde **déconnectée de votre système d'information**.

Exemple — Azur Services

Pour ses fichiers critiques, l'entreprise dispose :

Copie 1 → fichiers utilisés quotidiennement sur son environnement de travail

Copie 2 → sauvegarde automatique sur un environnement distinct

Copie 3 → sauvegarde supplémentaire conservée hors ligne

Ainsi, une attaque qui chiffre les fichiers accessibles depuis le réseau a moins de chances de détruire simultanément toutes les copies.

Votre situation

- ☐ J'ai plusieurs copies de mes données critiques.
- ☐ Elles ne dépendent pas toutes du même environnement.
- ☐ Au moins une sauvegarde est hors ligne et protégée.

⚠ **Vous ne cochez pas les trois cases ? →** Identifiez avec votre prestataire informatique comment compléter votre dispositif.

DIGITAL FlashUP

4. Automatisez les sauvegardes

Une sauvegarde qui repose uniquement sur la mémoire d'une personne finit souvent par être oubliée.

À faire →

☐ Programmer les sauvegardes automatiques lorsque c'est possible.
☐ Désigner une personne responsable du suivi.
☐ Vérifier que les sauvegardes prévues ont réussi.
☐ Activer une alerte en cas d'échec lorsque l'outil le permet.

Exemple — Azur Services

Les sauvegardes sont programmées automatiquement chaque nuit.

Le responsable administratif ne réalise donc pas manuellement les sauvegardes. En revanche, **chaque lundi matin**, il vérifie que les sauvegardes de la semaine précédente se sont correctement exécutées et signale toute anomalie au prestataire informatique.

Test express

Responsable chez vous : _____

Fréquence de contrôle : _____

Savez-vous si **la dernière sauvegarde prévue a réellement réussi** ?

☐ Oui ☐ Non → Vérifiez-la.

5. Protégez vos sauvegardes

Une sauvegarde contient souvent une grande partie des informations sensibles de l'entreprise. Elle doit donc elle-même être protégée.

☐ Accès limité aux personnes autorisées
☐ Comptes d'administration protégés
☐ Sauvegardes sensibles chiffrées lorsque nécessaire
☐ Copie séparée de l'environnement principal
☐ Supports physiques conservés dans un lieu sécurisé
☐ Sauvegardes hors ligne non connectées inutilement

Exemple — Le mauvais réflexe

Un collaborateur copie chaque vendredi les dossiers de l'entreprise sur un disque dur externe.

Mais il laisse ensuite le disque branché en permanence à son ordinateur.

En cas de ransomware, le disque peut lui aussi être compromis.

Le bon réflexe

Une fois la sauvegarde terminée et vérifiée, la copie destinée à rester hors ligne est **déconnectée et conservée dans un endroit sécurisé**.

6. Testez que vous savez réellement restaurer

> **Avoir une sauvegarde ne garantit pas que vous saurez récupérer vos données.**

Test de restauration en 5 minutes

1. Choisissez un fichier sauvegardé.
2. Restaurez-le dans un emplacement de test.
3. Ouvrez-le.
4. Vérifiez son contenu.
5. Notez la date et le résultat.

Exemple — Azur Services

Tous les trois mois, le responsable choisit au hasard :

- une facture ;
- un document client ;
- un fichier partagé.

Le prestataire les restaure depuis la sauvegarde.
L'entreprise vérifie ensuite qu'ils s'ouvrent normalement.

Dernier test : __ / __ / ____ ☐ Réussi ☐ Échec

Prochain test : __ / __ / ____

Pour vos systèmes les plus critiques, allez plus loin : vérifiez périodiquement que vous pouvez **remettre réellement le service en fonctionnement**, pas uniquement récupérer un fichier.

7. Définissez l'ordre de restauration

Après une cyberattaque, tout ne pourra pas nécessairement être restauré simultanément.

Posez-vous cette question :

> **Qu'est-ce qui doit fonctionner en premier pour que mon entreprise puisse reprendre son activité ?**

Exemple — Azur Services

Après réflexion, l'entreprise décide :

1. **Messagerie** → pouvoir communiquer
2. **Base clients** → retrouver les informations clients
3. **Gestion/facturation** → pouvoir facturer
4. **Fichiers opérationnels** → reprendre les dossiers en cours
5. **Archives** → peuvent attendre

Votre ordre :

1. _____
2. _____
3. _____
4. _____
5. _____

Cette réflexion constitue également une première étape vers votre **Plan de Continuité d'Activité (PCA)**.

Construisez maintenant votre politique de sauvegarde

À la fin de cette fiche, vous devez pouvoir remplir cette carte :

Question	Exemple Azur Services	Votre entreprise
Que sauvegardons-nous ?	Clients, facturation, contrats, fichiers, emails	_____
À quelle fréquence ?	Quotidienne pour les données critiques	_____
Où ?	Environnement de sauvegarde distinct	_____
Copie hors ligne ?	Oui	☐ Oui ☐ Non
Qui contrôle ?	Responsable administratif	_____
Quand testons-nous ?	Tous les 3 mois	_____
Que restaurons-nous en premier ?	Messagerie puis base clients	_____

Le test final

Posez cette question dans votre entreprise :

> **« Si nous perdons nos données aujourd'hui, quelle sauvegarde utilisons-nous, qui s'en occupe et que remettons-nous en fonctionnement en premier ? »**

Vous obtenez une réponse précise ?

- ☐ **Oui** → Testez maintenant que cette réponse fonctionne réellement.
- ☐ **Non** → Complétez les points manquants de cette fiche avec la personne ou le prestataire qui gère votre informatique.

Besoin d'aller plus loin ?

Consultez les ressources disponibles en Principauté sur **Cybermalveillance.gouv.mc** et rapprochez-vous de votre prestataire informatique pour adapter le dispositif à votre environnement.

DIGITAL FlashUP

DIGITAL FlashUP

RESTEZ CONNECTÉS

& Boostez vos compétences numériques sur MONENTREPRISE.GOUV.MC/EME

Gouvernement Princier
PRINCIPAUTÉ DE MONACO
Extended Monaco Entreprise
MONACO BUSINESS OFFICE