ANTENNE RÉGION VALAIS ROMAND

I.2 : SAUVEGARDES INFORMATIQUES

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

CONTEXTE

Les données informatiques ont une valeur capitale pour le bon fonctionnement de l'activité, une perte peut avoir des conséquences graves pour l'organisation.

Elément incontournable dans la stratégie numérique, la sauvegarde informatique permet de mettre en sécurité les données face à l'ensemble des risques auxquels les communes peuvent être exposées *(failles techniques, sinistres, cyberattaques, vols, actions humaines, etc.).*

Une personne clairement définie au sein de l'administration doit avoir la responsabilité des sauvegardes informatiques. L'annexe I.2.I fournit un cahier des charges type.

QUI ?

Exécutif communal

L'exécutif communal est responsable de la sécurité des données du système d'information de la commune. Il est donc en charge de nommer un responsable «sauvegarde» et de s'assurer que toutes les mesures basiques ont été prises.

Opérationnel communal

Un responsable des sauvegardes doit être nommé au sein de l'administration. Une formation générale **(CFC de commerce)** convient pour le rôle, mais une bonne compréhension des processus de la commune, ainsi qu'une affinité certaine avec l'informatique sont essentielles. Des compétences rédactionnelles sont nécessaires pour l'écriture et la revue des procédures. Des qualités d'écoute sont également souhaitées. Un niveau hiérarchique supérieur serait pertinent, notamment pour les tâches de contrôle. L'activité peut représenter **entre 5 et 15% d'un EPT** selon le nombre de collaborateurs dans la commune.

POINTS DE CONTRÔLE

- ☐ Nous avons une stratégie de sauvegarde clairement documentée dans un plan de sauvegarde.
- ☐ Un responsable des sauvegardes est nommé au sein de la commune et son cahier des charges est clair.
- ☐ Nous avons un contrat clair et à jour avec les prestataires gérant nos sauvegardes. Les responsabilités de chacun y sont clairement énoncées.
- ☐ Chaque 6 mois (au maximum), nous effectuons un test de récupération de nos sauvegardes.
- ☐ Nos sauvegardes existent de manière redondante, avec une version au moins séparée du réseau (en cas d'attaque ou de sinistre).
- ☐ Nous avons un inventaire des données à sauvegarder et des moyens d'y accéder.

ACTIONS PROPOSÉES

1. Nommer un responsable «sauvegarde des données»

Une personne clairement définie au sein de l'administration doit avoir la responsabilité des sauvegardes informatiques. Un cahier des charges complet est proposé en annexe I.2.I de la présente fiche.

2. Recenser les données critiques

Les données, leur localisation et le moyen d'y accéder doivent être référencés. Un support (tableau structuré) pour ce faire est fourni en annexe I.2.II de la présente fiche et est téléchargeable sur le site de l'Antenne.

Un support pour le recensement des données critiques est disponible sur l'extranet de l'Antenne Région Valais romand à l'adresse suivante: **https://www.regionvalaisromand.ch/fr/fiches-thematiques-provisoires-bonnes-pratiques-1813.html**

ou accessible grâce au QR code suivant:

3. Vérifier le contrat de prestations lié aux sauvegardes

Il s'agit de vérifier qu'il existe bien un contrat entre la commune et le prestataire IT qui stipule l'organisation des sauvegardes, ainsi que la définition claire des responsabilités. Une vue d'ensemble des bases nécessaires à un test de récupération réussi fournit une orientation à donner à ce contrat et est proposée en annexe I.2.III de la présente fiche.

ANTENNE RÉGION VALAIS ROMAND

I.2 : SAUVEGARDES INFORMATIQUES

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.
Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.

ACTIONS PROPOSÉES (SUITE)

4. Édicter une directive sur la sauvegarde des fichiers

Édicter une directive interne pour clarifier la discipline à adopter concernant les enregistrements des fichiers (trop de collaborateurs enregistrent des fichiers sur le disque dur local (propre à la machine), et ne sont ainsi pas sauvegardés). La procédure pour récupérer une donnée disparue doit également être connue de toutes et tous.

5. Tester la procédure de récupération des données

S'assurer de la règle du «3-2-1-0» : les données doivent exister en 3 copies, 2 formats, 1 copie hors du site et 0 erreur au test de récupération. L'annexe I.2.III résume les éléments principaux d'un test de récupération et l'annexe I.2.IV fournit un courrier type à envoyer aux prestataires externes pour lancer ce type de test.

6. S'assurer de la redondance / séparation des sauvegardes

Vérifier auprès du prestataire IT, par écrit, que les données sont séparées du réseau et redondantes (un ransomware peut s'attaquer aux sauvegardes). Un courrier type vous est proposé en annexe de la présente fiche.

ANNEXES / RÉFÉRENCES

I.2.I : Cahier des charges pour responsable sauvegardes
I.2.II : Support pour recensement des données critiques
I.2.III : Fiche pratique pour les tests de récupération des sauvegardes
I.2.IV : Textes pour courriers à envoyer aux prestataires

I : CAHIER DES CHARGES POUR RESPONSABLE SAUVEGARDES

Ce cahier des charges doit être considéré comme indicatif mais n'est en aucun cas exhaustif.

PROFIL

Le responsable de la sauvegarde des données devrait être défini dans l'organisation interne. Une bonne compréhension des processus de la commune est essentielle. Le responsable doit être à l'écoute et disposer d'un bon relationnel.

Une formation générale (CFC employé de commerce) convient pour le rôle : Des compétences rédactionnelles sont nécessaires pour l'écriture et la revue des procédures. Des connaissances en informatique sont un atout pour simplifier les échanges avec les prestataires. Le document « Sauvegardes : Pour approfondir – Glossaire et lien vers des articles complémentaires » (référence 1) propose une documentation accessible à tous. Des formations peuvent être dispensées par les fournisseurs de logiciels spécialisés (Veeam, Asigra, Acronis, etc.).

L'activité peut représenter entre 5 et 15% d'un équivalent plein temps selon le nombre de collaborateurs. Le travail se répartit entre établir et mettre à jour la documentation, réaliser les contrôles réguliers du bon fonctionnement des sauvegardes et assister les collaborateurs lors de la perte ponctuelle de données.

RESPONSABILITÉ ET CADRE LÉGAL

Le responsable des sauvegardes internes doit s'assurer que la copie des données fonctionne selon le processus défini. Le responsable doit informer et guider l'exécutif communal pour garantir le maintien du matériel et des prestations. Le présent document propose une liste d'actions à entreprendre pour accomplir cette mission.

L'exécutif a la responsabilité juridique des données traitées par ses services, en particulier des données à caractère personnel. Il doit mettre à disposition du responsable sauvegarde interne les moyens nécessaires à la protection des données de la commune.

TÂCHES MINIMALES

1. **Mettre en place une stratégie de sauvegarde** et la documenter dans un plan de sauvegarde.
   - S'assurer que les données soient efficacement sauvegardées, avec une redondance des sauvegardes et la protection de celles-ci. Cette prestation peut être réalisée en interne ou sous-traitée (cf. point 4).
   - Ce processus doit être documenté (référence 2), il doit définir des moyens de récupération rapides et efficaces ainsi que la fréquence des tests qui valident la bonne marche des systèmes.
2. **S'assurer du bon fonctionnement des sauvegardes** régulières des données essentielles.
   - Identifier les appareils, supports et logiciels qui contiennent des données et déterminer les données à sauvegarder. Un canevas d'inventaire des données est proposé en annexe.
3. **Tester la procédure de récupération des données :** S'assurer que la règle du 3-2-1-0 est maintenue.
   - 3 copies, 2 formats, 1 copie hors du site et 0 erreur lors des tests de récupération.

TÂCHES OPTIMALES

Sous-traiter la gestion des sauvegardes informatiques

Si l'organisation ne dispose pas de service informatique, la gestion technique des sauvegardes peut être complexe. L'organisation des sauvegardes peut être déléguée à un prestataire informatique. Il convient cependant de s'assurer que les rôles et responsabilités sont clairement établis.

4. **Vérifier les contrats de prestation liés aux sauvegardes :** Il s'agit de vérifier qu'il existe un contrat entre la commune et le prestataire IT qui stipule l'organisation des sauvegardes ainsi que les responsabilités.

I : CAHIER DES CHARGES POUR RESPONSABLE SAUVEGARDES

Ce cahier des charges doit être considéré comme indicatif mais n'est en aucun cas exhaustif.

TÂCHES OPTIMALES (SUITE)

Gérer ses sauvegardes informatiques en interne

La gestion interne des sauvegardes autorise plus de flexibilité et permet la maitrise complète de la gestion des données. De bonnes compétences en informatique sont cependant nécessaires pour garantir le bon fonctionnement des systèmes. Il est d'autre part impératif qu'à minima une sauvegarde hebdomadaire soit fortement protégée (cf. point 7).

5. **Choisir les solutions de sauvegarde** adaptées au besoin de l'organisation.
   - Sauvegardes internes ou externes (voir référence 1)
   - Sauvegarde totale, incrémentale ou différentielle (voir référence 1)
6. **Planifier les sauvegardes** selon les besoins opérationnels (en général, la nuit et le weekend).
7. **Protégez les données sauvegardées :** Conserver des copies en lecture seule, déconnecter le support utilisé, conserver les supports dans un lieu sûr.
   - S'assurer qu'il n'est pas possible pour une personne seule (y compris un administrateur) de détruire toutes les sauvegardes.
8. **Maintenir en condition opérationnelle,** gérer les évolutions ainsi que la gestion de la capacité des solutions de stockage et sauvegarde.
9. **Assurer la sauvegarde des logiciels indispensables** à l'exploitation des données.

Maintenance et discipline

Les utilisateurs du système jouent un rôle important dans la protection des informations. La sensibilisation aux risques de perte de données et le rappel des règles sont essentiels pour l'adhésion des collaborateurs.

10. **Maintenir et soutenir la directive sur la sauvegarde des fichiers :** Maintenir la directive interne pour l'enregistrement des fichiers (éviter les enregistrements en local), sensibiliser les utilisateurs et faire savoir comment récupérer des données disparues.

ANTENNE RÉGION VALAIS ROMAND

I.I.I: FICHE PRATIQUE POUR LES TESTS DE RÉCUPÉRATION DES SAUVEGARDES

Cette fiche doit être considérée comme indicative, mais n'est en aucun cas exhaustive. Rapprochez-vous de vos prestataires IT concernés pour adapter ce guide à leurs besoins.

QUI?

Responsable de la sauvegarde des données

Le responsable de la sauvegarde des données devrait être défini dans l'organisation interne. Il garantit que le bon fonctionnement des sauvegardes est testé régulièrement.

QUOI?

Les fichiers informatiques

La sauvegarde des fichiers informatiques nécessaires au bon fonctionnement de l'organisation doit être assurée en tout temps. Des tests de récupération de données doivent garantir son bon fonctionnement. Elles peuvent être le dernier rempart face à une attaque de cybercriminel. Un exemple de courrier est proposé en annexe I.

Les bases de données des systèmes d'information

Les données contenues dans certains logiciels représentent une ressource importante pour la bonne marche opérationnelle de l'organisation. Les systèmes d'information tels que ERP, CRM ou des systèmes spécifiques à l'activité peuvent contenir des informations confidentielles et/ou essentielles à l'organisation. Il convient de s'assurer qu'elles sont sauvegardées et qu'elles peuvent être restaurées rapidement en cas de besoin.

Par exemple, il est nécessaire de valider:

- la disponibilité du fournisseur du programme,
- si le logiciel peut être réinstallé dans l'état d'origine,
- si la version du logiciel est toujours supportée, maintenue,
- si les paramétrages propres à l'organisation sont sauvegardés.

La sauvegarde d'une image complète de votre serveur peut être assurée par certains outils (Veeam, Asigra, Acronis, etc.). qui vous permettront de récupérer votre environnement complet tel qu'il était lors de la dernière sauvegarde.

QUAND?

Un test de récupération de fichier devrait être réalisé au minimum chaque 6 mois.

Le bon fonctionnement des backups de vos systèmes d'information devrait être validé une fois par an.

La reconstitution des systèmes d'information à partir des sauvegardes peut être testée lors du déploiement d'un nouvel environnement, par exemple lors de la création d'un environnement de test, d'un changement de serveur ou d'un changement de version majeur du logiciel. Cette procédure devrait être réalisée tous les 4 ans au minimum. L'annexe I.2.IV vous propose des courriers type pour les prestataires IT.

IV: TEXTES POUR COURRIERS À ENVOYER AUX PRESTATAIRES

Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique. Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.

EXEMPLE DE COURRIEL POUR LES PRESTATAIRES

Objet: Vérification de la configuration de nos sauvegardes

Bonjour Monsieur Prestataire IT,

Dans le cadre de la revue de notre procédure de sauvegarde,
nous souhaiterions nous assurer des éléments suivants:

- L'intervalle de la sauvegarde de nos données est au minimum une fois par jour.
- Il est possible de restaurer l'état de notre système et de ses données à l'état d'il y a 3 mois.
- Le bon fonctionnement de la sauvegarde des données est contrôlé au moins une fois par semaine.
- Une copie des données existe dans un second emplacement hors feu ou inondation.
- Il n'est pas possible pour une personne seule (y.c. un administrateur) de détruire toutes les sauvegardes des données.

Je vous remercie pour votre retour et votre confirmation écrite.
Je reste à disposition pour toute question supplémentaire.

Meilleures salutations

Objet: Restauration du document «Exemple.docx»

Bonjour Monsieur Prestataire IT,

Dans le cadre de notre procédure de test, nous souhaiterions récupérer le document « Exemple.docx » qui a été effacé de notre dossier partagé.

Avant d'être supprimé, il était sauvegardé dans le dossier *K:/Projects/CyberSec/Documentation*

Lorsque vous avez récupéré le document, merci de m'indiquer où je peux trouver le fichier ainsi que la date de la sauvegarde restaurée.

Je vous remercie pour votre support et reste à disposition pour toute question.

Meilleures salutations

Objet : Validation de l'intégrité de la sauvegarde de notre ERP

Bonjour Monsieur X,

Dans le cadre de notre procédure de test, nous souhaiterions valider que le fichier de sauvegarde de notre ERP « export_full.dump »* est fonctionnel et permet de restaurer nos systèmes d'information.

Le fichier est sauvegardé dans le dossier du serveur ERP_ORA *c:\backup\export_full.dump*.

Veuillez confirmer que le fichier permet de remonter notre système avec l'intégralité des données de notre système.

Je vous remercie pour votre support et reste à disposition pour toute question.

Meilleures salutations

** Un dump est un anglicisme très souvent utilisé dans le monde informatique. Il désigne une opération informatique qui consiste à copier les informations d'une base de données dans un autre emplacement (serveur local, etc.) ou dans un fichier. Le dump informatique s'apparente aux sauvegardes de données ou aux copies de sécurité d'une base de données.*