POD Maatschappelijke Integratie
SPP Intégration Sociale

A Mesdames les Présidentes et à Messieurs les Présidents des centres publics d'action sociale et à leur DPD.

Avez-vous des questions ou souhaitez-vous des informations supplémentaires ?
Envoyez un courriel avec le DPD à l'adresse suivante MI.DPO@mi-is.be
Ou prenez contact avec lui au 02 508 84 30

Date : 7/12/2022

Instructions en matière de sauvegardes de données

afin de faire face à un événement grave impliquant la perte ou l'impossibilité d'accéder aux données de travail.

Madame la Présidente,
Monsieur le Président,

Les cyberattaques menacent tous les secteurs d'activité et les CPAS n'y échappent malheureusement pas. Des événements récents rappellent que les conséquences de ces attaques peuvent être désastreuses pour votre administration et par conséquent pour les ayants droit.

Le SPP Intégration Sociale vous informe de bonnes pratiques à adopter pour se prémunir au mieux contre les conséquences dévastatrices de telles attaques :

- D'abord en vous rappelant comment se préparer pour faire face à toute attaque, et quelles actions entreprendre en cas de survenance de l'attaque;
- Ensuite en vous rappelant comment mettre à l'abri ses données afin d'en assurer la disponibilité et l'intégrité, c'est-à-dire en disposant de sauvegardes correctement exécutées.

1. FAIRE FACE À UNE CYBERATTAQUE

Quelle que soit la taille de votre CPAS, il faut se préparer à une cyberattaque et prendre les mesures préventives adéquates.

1.1. DOCUMENTS UTILES

Pour vous y aider, il existe plusieurs recommandations faites par les instances publiques belges en charge de la cybersécurité. Nous vous invitons à consulter les informations publiées sur ces pages :

- https://cyberguide.ccb.belgium.be/fr et https://cyberguide.ccb.belgium.be/fr/prenez-main-securite
- https://www.cert.be/fr/conseils
  - et dans le cas très problématique des rançongiciels : https://www.cert.be/fr/paper/ransomware-protection-et-prevention

SPP Intégration Sociale, Lutte contre la Pauvreté, Economie Sociale et Politique des Grandes Villes
Centre administratif Botanique - Finance Tower
Boulevard du Jardin Botanique 50 boîte 165

Outre les mesures pratiques qui sont décrites dans ces documents, il vous est recommandé de disposer :

- D'une procédure de gestion des incidents (« security breach management policy »), afin d'identifier le plus rapidement possible l'incident et d'en avertir les personnes adéquates. Cette procédure sera élaborée par ou sous la supervision du DPD, puis soumise et validée par sa Direction,
- D'un plan de continuité d'activités (« business continuity plan » ou « BCP »), afin de protéger le cœur des activités en situation d'incident, au moins en mode dégradé. Le but ici est de limiter le dommage et de permettre à l'entreprise une reprise des activités « normales » au plus vite.
- D'un plan de reprise d'activités (« disaster recovery plan » ou « DRP »), pour permettre de relancer rapidement et complètement l'activité.

Vu l'importance des cyberattaques de type « rançongiciel » et vu les effets désastreux de celles-ci, nous vous recommandons de télécharger et de consulter le document disponible à l'adresse https://www.cert.be/sites/default/files/ransomware_2019_fr.pdf .
Il contient de précieux conseils et des informations diverses pour vous permettre d'organiser votre défense contre ces agressions particulièrement brutales et désastreuses.
D'autre part, le CCB (Centre pour la Cybersécurité Belgique) a publié un document particulièrement pratique qui reprend un plan d'actions en 12 points à exécuter sans tarder en cas d'attaque (https://cert.be/sites/default/files/steps_to_take_in_case_of_ransomware_attack_def_fr.pdf).

1.2. QUI PRÉVENIR EN CAS D'ATTAQUE ?

Pour rappel aussi, il y a obligation de notifier l'incident à une autorité de contrôle et/ou aux personnes potentiellement affectées par les conséquences de l'incident (par exemple, en vertu du RGPD et/ ou de la Directive NIS – et de sa transposition en loi belge).
En cas d'incident de sécurité, il faut donc se poser la question de savoir si votre CPAS est légalement tenu de le notifier ou pas.

4 ÉTAPES :

1° Identifier l'incident et enclencher la procédure interne de traitement des incidents
2° Identifier et respecter les obligations légales qui s'imposent à votre CPAS
3° Déposer plainte / signaler l'incident (https://www.cert.be/fr/signaler-un-incident)
4° Assurer une bonne communication de crise et préserver sa réputation

Pour information, quelques pointeurs vers des publications dont la lecture est hautement recommandée et pourrait aider à constituer votre propre plan de prévention et réponse en cas d'incident :

- Recommandations pour réaction immédiate en cas de cyberattaque: https://www.cert.be/fr/premiers-secours-en-cas-de-cyberattaque
- Conseils pour sauvegardes de données (source CCB) : https://cyberguide.ccb.belgium.be/fr/sauvegarde-restoration
- Guide sur les mesures à prendre en cas d'attaque de type « rançongiciel): https://cert.be/sites/default/files/steps_to_take_in_case_of_ransomware_attack_def_fr.pdf

2. GESTION DE LA SAUVEGARDE DES DONNÉES

De bonnes sauvegardes de données avec un plan éprouvé pour leur exécution sont indispensables pour éviter ou au moins minimiser l'impact d'une paralysie des systèmes et l'indisponibilité des informations, impliquant une interruption (ou à tout le moins une perturbation) des services :

- En cas de perte de données suite à une erreur (généralement humaine)
- En cas d'erreur de traitement ayant affecté un gros volume de données
- en cas de dégâts consécutifs à une cyberattaque, notamment celles causées par un Ransomware (rançongiciel).

Outre les garanties qu'un tel plan de sauvegarde apportera au niveau de disponibilité et d'intégrité des données, il vous permettra de poursuivre vos activités sans préjudices pour vos usagers et sans porter atteintes à la réputation de vos services.

Le plan de sauvegarde des données sera repris dans le cadre des plans de continuité des activités et de reprise après désastre (voir ci-dessous).

1.1. PRINCIPES

La définition d'un schéma de sauvegarde doit se baser sur un accord avec l'ensemble de l'organisation portant sur les durées acceptées concernant les données qui pourront être perdues (RPO) et le temps pour une reprise d'un travail normal (WRT).

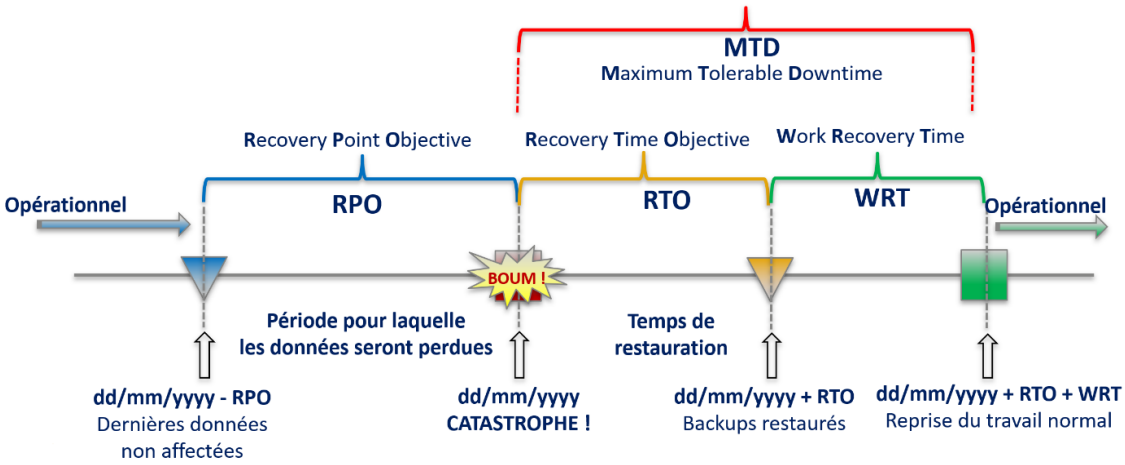
Cet accord peut être formalisé dans un contrat de service (Service Level Agreement ou « SLA ») lorsque la sauvegarde est gérée par prestataire de service en sous-traitance)

Les termes ci-dessous sont généralement utilisés pour définir les paramètres des sauvegardes à effectuer,

RPO : Recovery Point Objective :
La période maximale autorisée pour laquelle le CPAS accepte que les données puissent être perdues
RTO : Recovery Time Objective :
Le temps maximum autorisé pour réaliser une restauration à partir d'une sauvegarde
WRT: Work Recovery Time:
Période nécessaire après restauration des données pour tout réconcilier et retrouver un contexte complet et opérationnel pour les activités normales du CPAS

Ces paramètres seront détaillés dans un document formel conclu avec l'entité (interne ou externe) responsable de ces sauvegardes et mentionnera les accords suivants :
SLA : Service Level Agreement :
contrat entre client et fournisseur dans lequel sont consignés tous les accords, tels que objectifs à atteindre en termes de disponibilité et de performances, services de veille, coûts, gestion des incidents, personnes de contact, ...
SLO : Service Level Objective :
décrit dans le SLA les objectifs techniques mesurables tels que RPO, RTO (voir ci-dessus).

Le schéma suivant met en relation ces divers paramètres sur une ligne du temps.



1.2. QUELLES DONNÉES SAUVEGARDER?

Le CPAS traite des données au moyen de systèmes gérés soit par son propre personnel, soit par un (ou plusieurs) sous-traitant(s) informatique(s).

On trouvera ainsi :

- les producteurs de logiciels
- Les services informatiques de la ville ou de la commune dont dépend le CPAS
- Un service dans le Cloud.

Dans ces cas, les sauvegardes sont prises en charge par ces sous-traitants dans le cadre du contrat conclu entre le sous-traitant et le CPAS, responsable du traitement.

Les informations fournies dans la suite permettront au DPD du CPAS de s'assurer de disposer des garanties suffisantes de la part aussi bien de ses sous-traitants que de la ou les personnes en charge d'une prise en charge locale de sauvegarde de données locales.

REMARQUE IMPORTANTE : les informations qui suivent sont principalement destinées au CPAS qui doit effectuer lui-même les sauvegardes nécessaires afin de pouvoir réduire, voire éliminer l'impact d'une cyberattaque.

Types de données :

Les données à sauvegarder seront traitées différemment, **selon leur nature**, idéalement, selon une classification conforme aux standards repris dans la Norme Minimale de la BCSS (https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_data_classification_donnees.pdf).

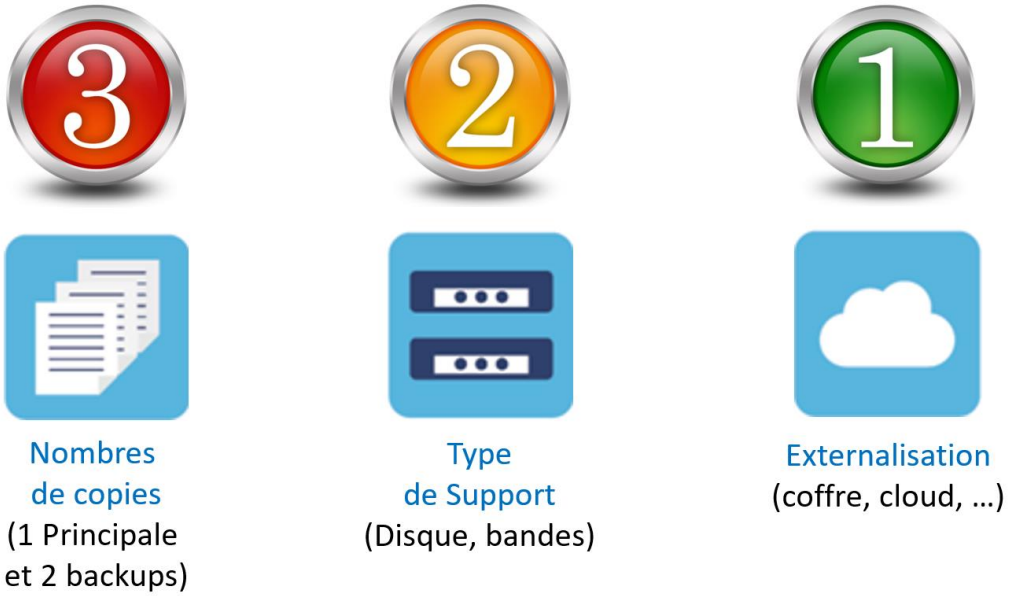
On distinguera au minimum les 3 types de données suivants:

- Données « Système »;
- Données non-sensibles mais importantes dans le cadre des activités quotidiennes du CPAS;
- Données à caractère personnel. Ces dernières exigent d'ailleurs des précautions et dispositions particulières afin de se conformer aux exigences en matière de RGPD.

1.3. STRATÉGIE ET TYPES DE SAUVEGARDES

La stratégie « 1-2-3»

La stratégie recommandée correspondra au schéma suivant :



Il est essentiel de prévoir une sauvegarde externe pour éviter la contamination des fichiers de sauvegarde en cas par exemple de ransomware.

Il existe essentiellement 3 types différents de plan de sauvegarde.

Types de plan de sauvegarde

La sauvegarde complète

Une sauvegarde complète, enregistre chaque fois une copie complète des bases de données, fichiers et informations du système informatique selon une périodicité programmée.
Bien que le temps de sauvegarde soit plus lent et que la sauvegarde nécessite plus d'espace de stockage, l'avantage de la sauvegarde complète est que les opérations de restauration sont plus rapides et plus simples.

La sauvegarde incrémentale

La sauvegarde initiale est complète puis, lors de chaque sauvegarde suivante, on ne stocke que les modifications apportées depuis la dernière sauvegarde.

La sauvegarde est plus rapide puisqu'il y a moins de données à sauver. C'est donc aussi la méthode qui nécessite le moins de volume de stockage, mais la restauration des données est plus longue.

La sauvegarde différentielle

Comme avec la méthode incrémentale, la première sauvegarde est complète. Mais par la suite, le système sauvegarde tous les changements depuis la dernière sauvegarde **complète**. Ce type de sauvegarde nécessite plus d'espace de stockage que l'incrémentale, mais permet un temps de restauration plus rapide.

Rotation des supports de sauvegarde

Les sauvegardes sont réalisées selon un schéma de rotation des supports qui en indique le modèle, leur fréquence et le modèle de rotation, tel que:

Premier entré, premier sorti (FIFO)
On enregistre les nouveaux fichiers ou les fichiers modifiés sur le support qui contient les données sauvegardées les plus anciennes - et donc les moins utiles. C'est le schéma de rotation le plus simple.

> ***Exemple : chaque sauvegarde est réalisée sur un support différent ; u****ne sauvegarde quotidienne sur un ensemble de 14 supports apporte une profondeur de sauvegarde de 14 jours.*
>
> *Chaque jour, c'est le support qui contient les informations les plus anciennes qui est inséré lors de l'exécution de la sauvegarde. .*

Grand-père – père - fils
i y a au moins trois cycles de sauvegarde : quotidien, hebdomadaire et mensuel.

- Les sauvegardes quotidiennes utilisent des supports en mode alterné comme décrit ci-dessus).
- Les sauvegardes hebdomadaires sont également alternées sur une base hebdomadaire
- la sauvegarde mensuelle est réalisée sur une base mensuelle.

On peut également prévoir des sauvegardes séparées pour le plus longues périodes : trimestrielles, semestrielles et/ou annuelles .

C'est le schéma de rotation le plus courant pour les supports de sauvegarde.

D'autres méthodes existent encore (p.ex. « La Tour de Hanoï ») : elles ont toutes pour vocation d'optimiser le cycle de sauvegarde.

1.4. PLAN ET PROCÉDURE DE SAUVEGARDE

Comme repris dans toutes les recommandations, il est nécessaire de documenter l'approche adoptée pour réaliser les sauvegardes. Cette documentation consiste en un plan de sauvegarde élaboré par ou sous la supervision du DPD, convenu et validé par sa Direction, ainsi que la description de la ou des procédures décrivant en détails tous les paramètres et manipulations à réaliser pour la prise des sauvegardes.

Cette documentation permettra une transmission aisée et univoque lors de tout transfert de responsabilité, en cas d'absence, de départ, etc.

Le plan de sauvegarde indiquera:

- La liste des données (et leur type) prises en compte pour la sauvegarde ;
- le modèle de sauvegarde (« Complet », Incrémental », « Différentiel ») et leur schéma de rotation;
- la procédure précisant les intervenants, leurs actions et responsabilités respectives et les vérifications régulières à exécuter ;
- les moyens de stockage et leur gestion (accès, manutention, lieu, …);
- les procédures de test de restauration avec tests de validité ;
- la destruction de tous les supports ayant contenu des données.

Les journaux (« logs »), conservés avec les supports de sauvegardes, comporteront au minimum les informations suivantes :

- références du dispositif de sauvegarde ;
- périmètre ou composants concernés ;
- type de sauvegarde ;
- fichiers sauvegardés ;
- date de la sauvegarde ;
- statut de la sauvegarde.

1.5. SAUVEGARDES « IN-SITU » DE DONNÉES LOCALES

Lorsque le CPAS traite des données qui lui sont indispensables pour la continuité de ses activités sans que la sauvegarde soit réalisée par des fournisseurs de services informatiques, il lui faudra alors définir et mettre en œuvre les plans, procédures et moyens de sauvegarde utilisés en local.

Sauvegarder des fichiers à partir d'un PC vers un disque dur externe

En pratique, la technologie actuelle de disques durs externes connectés via USB 3.0 présente pour un coût relativement modique des possibilités de sauvegarde rapide et facile, tout en supportant les recommandations, types et rotations présentées ci-dessus.

Solution logicielle pour backup:

Il existe de nombreuses solutions, aussi bien en mode payant qu'en mode « FOSS » (Free Open-Source Software), selon les besoins attendus en matière de support.

Type de sauvegarde recommandé

Le type de sauvegarde qui semble le plus recommandé afin d'éviter de trop grands volumes à transférer tout en offrant assez de granularité est un **schéma** de sauvegarde « **complet + incrémental** ».

En règle générale, on considère qu'un schéma « complet plus différentiel » est plus approprié pour de plus grandes structures disposant de moyens informatiques plus larges.

Schéma de rotation recommandé

Le schéma de rotation préconisé est le « **Grand-père – père – fils** ». Même si les possibilités de restauration sont plus lentes, le volume de stockage nécessaire est largement inférieur et donc la possibilité de pouvoir conserver des copies plus anciennes beaucoup plus grande, ce qui dans certains cas peut-être une opportunité.

Il faut impérativement, dans tous les cas, prendre des mesures pour qu'un jeu de données soit stocké hors CPAS -, par exemple dans un coffre-fort de la Commune/Ville dont dépend le CPAS

… et bien sûr, documenter par des plans et procédures, former tous les acteurs et procéder régulièrement à des tests de restauration afin de s'assurer que l'ensemble est sous contrôle et fonctionne comme attendu.

Faut-il chiffrer les données lors de leur sauvegarde ?

Les données classifiées comme « confidentielles » ou « sensibles » seront préalablement chiffrées afin que tout vol de disque exclue la possibilité de récupérer ces données. La solution la plus simple et sans coût supplémentaire est d'utiliser « Bitlocker » de Microsoft pour verrouiller les disques.

Cloud ou pas Cloud ?

Une sauvegarde sur le Cloud, probablement plus coûteuse, exigera de plus que les données classifiées comme « confidentielles » ou « sensibles » soient nécessairement préalablement chiffrées.

Avez-vous encore une question au sujet des cyberattaques ou de la prise de sauvegarde de vos données? Prenez alors contact avec le SPP Intégration sociale, Lutte contre la pauvreté et Politique des grandes villes

- Par mail : MI.dpo@mi-is.be
- Par téléphone : + 32 2 508 85 86 de 8 h 30 à 12 h 30 et de 13 h à 16 h 30 (vendredi jusqu'à 16 h)

Je vous prie de croire, Mesdames les Présidentes, Messieurs les Présidents, en l'assurance de ma considération distinguée.

Signé

Alexandre LESIW
Président