Sauvegarde de l’information

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

**6. Exigences de la norme ISO 27001 : 2022**

**7. Politique sauvegarde de l’information**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

La politique sauvegarde de l’information a pour objet de montrer les méthodes que nous utilisons pour dupliquer et mettre en sécurité les données opérationnelles de nos systèmes informatiques.

**2. Finalité**

La politique sauvegarde de l’information a pour finalité de permettre la récupération après la perte de données ou de systèmes.

**3. Domaine d’application**

La politique sauvegarde de l’information s’applique à toutes les données opérationnelles utilisées dans notre organisation.

**4. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de la politique sauvegarde de l’information. Il est garant de son application. Il a l’appui du directeur.

**5. Documents**

Plan de sauvegarde

Sauvegarde

Activités de surveillance

Plan de gestion des incidents

Plan de continuité d’activité

Continuité d’activité

Utilisation des services en nuage

Suppression de l’information

**6. Exigences de la norme ISO 27001 : 2022**

A.8.13 Sauvegarde de l’information

Des copies de sauvegarde de l'information, des logiciels et des systèmes doivent être conservées et testées régulièrement selon la politique sauvegarde de l’information qui a été convenue.

**7. Politique sauvegarde de l’information**

La politique sauvegarde de l’information est établie afin de répondre aux exigences de l'organisation en matière de conservation des données et de sécurité de l’information.

Des installations de sauvegarde adéquates sont fournies afin de garantir que toutes les informations et tous les logiciels essentiels peuvent être récupérés à la suite d'un incident, d'une panne ou d'une perte de supports de stockage.

Le Plan de sauvegarde est élaboré et appliqué et concerne la sauvegarde de l’information, des logiciels et des systèmes.

Les sauvegardes sont protégées par des mécanismes de haute sécurité contre toute modification non autorisée.

Le plan de sauvegarde prend en compte les éléments suivants :

* produire des enregistrements précis et complets des copies de sauvegarde et des procédures de restauration documentées selon la procédure Sauvegarde
* décider de réaliser des sauvegardes complètes ou partielles selon la criticité de l’information
* choisir la fréquence des sauvegardes
* stocker les sauvegardes dans un lieu sûr, sécurisé et distant du site principal, protégé des risques :
  + d'intrusion
  + d’incendie
  + de dégâts des eaux
* donner aux informations de sauvegarde un niveau approprié de protection physique et environnementale conforme aux normes appliquées sur le site principal
* tester régulièrement les supports de sauvegarde
* tester la capacité à restaurer les données sauvegardées sur un système de test indépendant (et non en écrasant le support de stockage d'origine)
* protéger les sauvegardes au moyen d'un cryptage en fonction des risques identifiés (niveau élevé de confidentialité)
* s'assurer que la perte de données par inadvertance est détectée avant que la sauvegarde ne soit effectuée

Les procédures opérationnelles surveillent l'exécution des sauvegardes et traitent les échecs des sauvegardes planifiées selon la procédure Activités de surveillance.

Les mesures de sauvegarde pour les systèmes et services individuels sont régulièrement testées afin de s'assurer qu'elles répondent aux objectifs des plans de réponse aux incidents et de continuité des activités, cf. le Plan de gestion des incidents et Plan de continuité d’activité.

Dans le cas de systèmes et services critiques, les mesures de sauvegarde couvrent toutes les informations, applications et données du système nécessaires pour restaurer le système complet en cas de sinistre selon la procédure Continuité d’activité.

Pour les services en nuages, des copies de sauvegarde des informations, des applications et des systèmes de l'organisation dans l'environnement du service en nuage sont réalisées. Cette activité est surveillée régulièrement selon la politique Utilisation des services en nuage.

La période de conservation des informations commerciales essentielles est déterminée en tenant compte des exigences applicables.

La suppression de l’information sur les supports de stockage utilisés pour la sauvegarde une fois la période de conservation des informations expirée tient compte de la législation et des réglementations en vigueur, cf. le fichier Suppression de l’information.

Pour savoir ce que l’on doit sauvegarder, le mieux est de commencer par dresser une cartographie précise. Cela permet ensuite de vérifier l’efficacité des restaurations.

La politique sauvegarde de l’information définit :

* les données à sauvegarder
* la fréquence des sauvegardes
* la nature de sauvegarde :
  + totale
  + différentielle
  + ponctuelle
* la durée de conservation
* le type de sauvegarde approprié selon la classification de l’information
* les emplacements :
  + supports mobiles :
    - disque dur
    - clé USB
    - DVD
  + sur Internet (*cloud*)
* les mesures de protection
* la procédure de restauration
* les tests périodiques des supports de sauvegarde
* les tests périodiques de restauration

Exemples de domaines à inclure :

* bases de données
* serveurs de fichiers
* serveurs virtuels
* serveurs physiques
* équipements sensibles de l’infrastructure comme :
  + cœurs de réseau
  + routeurs centraux
  + répartiteurs de charge
  + pare-feu

Les données sauvegardées sont listées dans le fichier Plan de sauvegarde :

* les données applicatives
* les programmes
* les bibliothèques de programmes source
* les paramètres de configuration des :
  + applications
  + logiciels de base
* les serveurs métier
* l'ensemble des configurations des équipements réseau et sécurité
* les données utilisateurs
* l'ensemble des paramètres de configuration des postes utilisateurs

Fréquence de sauvegarde suggérée : quotidienne/hebdomadaire/mensuelle.