Sauvegarde

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

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

**5. Déroulement**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de permettre la récupération après la perte de données ou de systèmes.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Sauvegarde » s’applique aux personnes ayant accès aux outils de sauvegarde de l’information, des logiciels et des systèmes.

**1.3 Glossaire**

RSI – responsable sécurité de l’information

**2. Responsabilité**

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

**3. Documents**

Sauvegarde de l’information

Plan de sauvegarde

Plan de gestion des incidents

Plan de continuité d’activité

Sécurité de l’information avec les fournisseurs

Plan de classification

Suppression de l’information

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

A.8.13 Sauvegarde

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

**5. Déroulement**

La politique Sauvegarde de l’information établit les exigences de conservation des données.

Des installations de sauvegarde adéquates sont mises en place afin de garantir que toutes les données et tous les logiciels essentiels peuvent être récupérés suite à un incident, une panne ou une perte de support de stockage.

Le Plan de sauvegarde établit la façon dont l'organisation sauvegardera les informations, les logiciels et les systèmes selon la politique de Sauvegarde de l’information.

Le Plan de sauvegarde prend en compte les éléments suivants :

* produire des enregistrements précis et complets des copies de sauvegarde selon des activités documentées
* considérer :
  + les exigences commerciales de l'entreprise
  + les exigences de sécurité de l’information
  + la criticité de l’information
  + la fréquence des sauvegardes
* stocker les sauvegardes dans un lieu distant sûr et sécurisé
* donner aux informations de sauvegarde un niveau approprié de protection physique et environnementale selon les normes appliquées sur le site principal
* tester régulièrement les supports de sauvegarde afin de s’assurer qu’ils peuvent être utilisés en cas d'urgence
* 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 (confidentialité des données)
* s'assurer que la perte de données par inadvertance est détectée avant la sauvegarde

Les activités opérationnelles surveillent l'exécution des sauvegardes et traitent les échecs des sauvegardes planifiées afin de garantir l'exhaustivité des sauvegardes.

Les mesures de sauvegarde pour les systèmes et services individuels sont régulièrement testées pour s'assurer qu'elles répondent au Plan de gestion des incidents et au Plan de continuité d’activité.

Dans le cas de systèmes et services critiques, les mesures de sauvegarde incluent toutes les informations, applications et données du système nécessaires pour restaurer le système complet en cas de sinistre.

Lorsque l'organisation utilise un service en nuage, des copies de sauvegarde des informations, des applications et des systèmes sont réalisées de manière planifiée, cf. le fichier Sécurité de l’information avec les fournisseurs.

La période de conservation des informations sauvegardées est établie selon le Plan de classification. L’enregistrement des suppressions est conservé dans le fichier Suppression de l’information et tient compte de la législation et des réglementations applicables.