Programmes utilitaires privilégiés

**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 d'assurer que l'utilisation de programmes utilitaires n'endommage pas les mesures de sécurité du système et des applications de sécurité de l'information.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Programmes utilitaires privilégiés » s’applique aux personnes ayant un accès privilégié aux programmes utilitaires ayant la capacité de contourner les mesures de sécurité des systèmes et des applications à l’information et aux autres actifs de l’organisation.

**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**

Restriction d’accès

Authentification

Autorisations privilégiées

Séparation des environnements

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

A.8.18 Programmes utilitaires privilégiés

L'utilisation des programmes utilitaires ayant la capacité de contourner les mesures de sécurité des systèmes et des applications doit être limitée et contrôlée.

**5. Déroulement**

Les éléments suivants pour l'utilisation de programmes utilitaires capables de contourner les mesures du système et des applications sont pris en compte :

* limiter l'utilisation des programmes utilitaires à un nombre pratique minimum d'utilisateurs autorisés et de confiance, cf. la procédure Restriction d’accès
* utiliser l'identification, l'authentification et l'autorisation pour les programmes utilitaires, cf. la procédure Authentification
* définir et documenter les niveaux d'autorisation pour les programmes utilitaires dans le fichier Autorisations privilégiées
* autorisation d'utilisation spécifique pour un programme utilitaire
* ne pas mettre les programmes utilitaires à la disposition des utilisateurs qui ont accès aux applications sur les systèmes où la séparation des tâches est requise, cf. la procédure Séparation des environnements
* supprimer ou désactiver tous les programmes utilitaires inutiles
* séparer, au minimum, les programmes utilitaires des logiciels d'application. Dans la mesure du possible, séparer les communications réseau pour ces programmes du trafic des applications
* limiter la disponibilité des programmes utilitaires (pendant la durée d'une modification autorisée)
* enregistrer les journaux de toute utilisation de programmes utilitaires

La plupart des systèmes d'information ont un ou plusieurs programmes utilitaires capables de remplacer les contrôles du système et des applications comme :

* les diagnostics
* les correctifs
* les antivirus
* les défragmenteurs de disque
* les débogueurs
* les outils de sauvegarde et de réseau