Gestion des réseaux

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Enregistrements**

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

**7. Politique de gestion des réseaux**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2023 |
| **Page** | **Changement** | **Date** |

**1. Objet**

La politique de gestion des réseaux a pour objet d’identifier les exigences à respecter et les mesures de protection à effectuer sur les réseaux.

**2. Finalité**

La politique de gestion des réseaux a pour finalité de garantir la protection de l’information sur les réseaux de tout accès non autorisé.

**3. Domaine d’application**

La politique de gestion des réseaux s’applique à tous ceux qui accèdent aux réseaux et systèmes informatiques de 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 de gestion des réseaux. Il est garant de son application. Il a l’appui du directeur et de tous les responsables de département.

**5. Enregistrements**

Protection des réseaux

Accord fournisseur

Sauvegarde des informations

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

A.8.20 Sécurité des réseaux

Les réseaux et les terminaux réseau doivent être sécurisés, gérés et contrôlés pour protéger les informations des systèmes et des applications.

A.8.21 Sécurité des services réseau

Les mécanismes de sécurité, les niveaux de service et les exigences de services des services réseau doivent être identifiés, mis en oeuvre et surveillés.

A.8.22 Cloisonnement des réseaux

Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés dans les réseaux de l'organisme.

**7. Politique de gestion des réseaux**

La responsabilité de la gestion des équipements réseau est séparée de la responsabilité de la gestion des ordinateurs.

Des mesures spécifiques afin de préserver la confidentialité, l’intégrité et la disponibilité des données transmises sur les réseaux publics et les réseaux sans fil sont appliquées. Les serveurs sont physiquement situés dans un environnement à accès contrôlé.

La version du système d'exploitation de chaque réseau est à jour et suivie par le responsable réseau.

Les actions de prévention de la sécurité de l’information sur les réseaux sont définies et enregistrées dans le fichier Protection des réseaux.

La capacité du fournisseur de services de réseau à gérer ses services de façon sécurisée est surveillée régulièrement. Plus de détails dans la politique Relations avec les fournisseurs.

Dans le fichier Accord fournisseur le droit d’auditer le fournisseur est spécialement noté.

Le réseau local virtuel (VLAN – *Virtual Local Area Network*) est un réseau logique indépendant et coexiste avec le réseau physique.

L’accès entre les différents domaines du réseau est contrôlé au niveau du périmètre via une passerelle (pare-feu ou un routeur-filtre).

L’accès aux ressources locales et réseau demande une identification autorisée et un mot de passe.

Les critères de cloisonnement des réseaux en domaines et les accès autorisés sont déterminés en tenant compte des exigences de sécurité propres à chaque domaine, la politique de Contrôle d’accès et la procédure Classification et marquage de l’information.

Les configurations réseaux entrent dans le fichier Sauvegarde des informations afin de répondre à un cas de sinistre.