politique de sécurité du réseau

 Modèle

# Autorité et révision

## Contrôle et révision des documents

|  |  |
| --- | --- |
| **Vérification des documents**  |  |
| Auteur  |  |
| Propriétaire |  |
| Date de création |  |
| Dernière révision par  |  |
| Date de la dernière révision |  |

.

## Gestion des versions

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Date d'approbation** | **Approuvé par**  | **Description du changement** |
| 1.0 |  |  |  |

# Intro

La sécurité du réseau au sein de l'organisation est importante car elle constitue votre première défense contre les attaques extérieures. En mettant en œuvre des mesures techniques et organisationnelles efficaces en matière de sécurité des réseaux, vous pouvez empêcher les cybercriminels de cartographier votre infrastructure, de perturber vos communications, de collecter illégalement des données ou d'atteindre des applications et des appareils critiques.

Le présent document fait partie d'un ensemble de documents destinés à aider **[l'organisation]** à mettre en place une stratégie solide en matière de cybersécurité.

# Sécurité des réseaux

## Sécurité physique

Les composants du réseau, tels que les pare-feu et les commutateurs, doivent être placés dans des armoires dédiées. L'accès à ces armoires doit être réservé au personnel spécialement désigné. Les câbles de données et d'alimentation doivent être protégés contre les dommages.

## Séparation des réseaux

Pour empêcher les logiciels malveillants et autres abus de se propager sur le réseau, celui-ci doit être conçu comme une topologie séparée. Les systèmes doivent résider dans des VLAN désignés, séparés par des règles d'accès au pare-feu.

Les règles suivantes de séparation des VLAN doivent être respectées :

* Les systèmes fournissant des services en ligne (c'est-à-dire acceptant le trafic entrant de l'internet) doivent être séparés des autres systèmes.
* La gestion du réseau se fait via un VLAN séparé.
* Les systèmes fournissant des services connectés (c'est-à-dire acceptant un trafic entrant en provenance de réseaux non fiables autres que l'internet) doivent être séparés des autres systèmes.
* Les appareils des utilisateurs finaux doivent être séparés des serveurs.
* Les appareils non gérés doivent être séparés des appareils gérés.
* Les systèmes ayant des objectifs différents doivent être séparés.
* Les sites physiques doivent être séparés.
* Les systèmes de développement, de test et de production doivent être séparés.

## Pare-feu

Les VLAN doivent être séparés par des pare-feu. Le trafic réseau entre les VLAN et le trafic en provenance ou à destination de réseaux non fiables doivent être bloqués, sauf s'il est explicitement demandé qu'ils soient ouverts. L'accès sortant à l'internet pour les VLAN des utilisateurs du bureau est autorisé, à moins qu'il ne nuise à la sécurité ou aux performances de l'entreprise. Le trafic peut être hiérarchisé, par exemple pour éviter que les flux vidéo ou musicaux n'affectent le trafic bureautique lié au travail.

VPN

Pour le télétravail ou les communications de machine à machine sur des réseaux non fiables, le VPN peut être utilisé pour crypter le trafic réseau qui n'est pas crypté par défaut.

L'accès au RPV, et donc à tous les systèmes sous-jacents de l**'[Organisation],** doit, dans la mesure du possible, être configuré de manière à utiliser une forme d'authentification multifactorielle, de sorte qu'une personne non autorisée en possession d'informations d'identification compromises de l'[**Organisation]** ne puisse pas utiliser le RPV de l**'[Organisation].**

## Sécurisation des réseaux câblés

# Les ports du réseau doivent être protégés contre les dispositifs non fiables. Lorsque la sécurité physique est faible, des techniques de sécurité réseau telles que le filtrage MAC ou la sécurité d'accès au réseau doivent être utilisées pour bloquer ou isoler les dispositifs non fiables.

## Sécurité des réseaux sans fil

Le Wi-Fi utilise différentes normes pour le cryptage et l'authentification. Les méthodes ci-dessous sont classées par ordre de sécurité (la première est la seule méthode sûre) :

1. WPA2 + AES
2. WPA + AES (non préférée)
3. WPA + TKIP (non préférée)
4. WEP (ne jamais utiliser)
5. Réseau ouvert (jamais utilisé)

L'accès des utilisateurs doit être vérifié. Pour l'authentification des réseaux WIFI, il est préférable de disposer d'une base de données centrale d'utilisateurs par nom. La plupart des points d'accès WIFI des entreprises prennent en charge les protocoles LDAP ou RADIUS.

Les appareils non gérés ne doivent accéder qu'aux **[réseaux WIFI dédiés aux invités].** Il convient d'empêcher le trafic réseau entre les réseaux invités et ceux gérés par **[l'organisation].**

# Gestion du réseau

* Un schéma de réseau de haut niveau est élaboré et stocké (imprimé) en toute sécurité. Ce schéma comprend la description du matériel et des fonctions, ainsi que l'adressage (IP) nécessaire. Ce schéma est régulièrement mis à jour.
* Les ports de gestion doivent être réservés au personnel autorisé et ne doivent pas être connectés à l'internet, sauf via un VPN.
* L'accès des utilisateurs aux ports de gestion doit être contrôlé régulièrement. Il est préférable de disposer d'une base de données centrale d'utilisateurs par nom pour l'authentification de l'accès à la gestion.
* L'installation ou la modification de dispositifs de réseau doit être effectuée par ou en consultation avec le service informatique de **[l'organisation].**
* Les dispositifs d'infrastructure de réseau sont dotés d'une fonction de journalisation, axée sur la surveillance et le contrôle des flux de trafic à travers les zones du réseau et les différents niveaux de confiance. Les exemples incluent les événements importants pour l'administrateur tels que la connexion, les changements de système, les réinitialisations de mot de passe...
* Pour garantir la disponibilité et la performance des systèmes critiques et confidentiels, il convient d'envisager l'existence d'accords de niveau de service (SLA) pour ces composants du réseau.