Utilisation de la cryptographique

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

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

**7. Politique utilisation de la cryptographie**

Historique

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

**1. Objet**

La politique utilisation de la cryptographie a pour objet l’utilisation correcte de systèmes et techniques cryptographiques approuvés.

**2. Finalité**

La politique utilisation de la cryptographie a pour finalité d’assurer une utilisation appropriée et efficace de la cryptographie pour protéger la confidentialité, l'authenticité ou l'intégrité de l’information conformément aux exigences de l’organisation et de sécurité de l'information, et en tenant compte des exigences légales, statutaires, réglementaires et contractuelles liées à la cryptographie.

**3. Domaine d’application**

La politique utilisation de la cryptographie s’applique aux actifs de notre organisation et plus spécialement aux informations dites sensibles.

**4. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de la politique utilisation de la cryptographie. Il est garant de son application. Il a l’appui de la direction et de tous les responsables de département.

**5. Documents**

Utilisation de la cryptographie

Clés cryptographiques

Liste des exigences

Relations avec les fournisseurs

Règles disciplinaires

Appliquer la discipline

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

A.8.24 Utilisation de la cryptographie

Des règles pour l'utilisation efficace de la cryptographie, notamment la gestion des clés cryptographiques, doivent être définies et mises en œuvre.

**7. Politique utilisation de la cryptographie**

La politique utilisation de la cryptographie est validée par la direction.

Lors de l'utilisation de la cryptographie, les éléments suivants sont pris en compte :

* respecter les principes généraux de protection de l’information selon la procédure Utilisation de la cryptographie
* éviter une utilisation inappropriée ou incorrecte en maximisant les avantages et minimisant les risques de l'utilisation de techniques cryptographiques
* identifier le niveau de protection requis et la classification de l’information et, par conséquent, établir le type, la force et la qualité des algorithmes cryptographiques requis
* utiliser la cryptographie pour la protection des informations détenues sur les terminaux ou les supports de stockage mobiles et transmises sur les réseaux
* gérer les clés cryptographiques, cf. Clés cryptographiques :
  + génération et protection des clés cryptographiques
  + récupération des informations chiffrées en cas de clés perdues, compromises ou endommagées
* attribuer les rôles et responsabilités pour :
  + la mise en œuvre des règles d'utilisation efficace de la cryptographie
  + la gestion des clés, y compris la génération des clés
* adopter les normes et les algorithmes cryptographiques, la force de chiffrement, les solutions cryptographiques et les pratiques d'utilisation approuvées ou requises dans l'organisation
* gérer l'impact de l'utilisation d'informations cryptées sur les mesures de l'inspection du contenu (détection de logiciels malveillants ou filtrage de contenu)
* les réglementations et restrictions sur l'utilisation des techniques cryptographiques et les problèmes de flux transfrontalier d'informations cryptées, cf. la Liste des exigences

Le contenu des accords (ou contrats) avec des fournisseurs externes de services cryptographiques incluent les questions de responsabilité, de fiabilité des services et de temps de réponse pour la fourniture des services selon la procédure Relations avec les fournisseurs.

La gestion appropriée des clés cryptographiques nécessite des règles sécurisées pour les :

* générer
* stocker
* archiver
* récupérer
* distribuer
* retirer
* détruire

Le système de gestion des clés cryptographiques est basé sur un ensemble convenu de normes, de procédures et de méthodes sécurisées pour :

* générer des clés pour différents systèmes cryptographiques et différentes applications
* délivrer et obtenir des certificats de clé publique
* distribuer les clés aux entités prévues et les règles comment activer les clés lorsqu'elles sont reçues
* stocker les clés et la manière dont les utilisateurs autorisés obtiennent l'accès aux clés
* changer ou mettre à jour les clés et les règles sur le moment de changer les clés et comment cela sera fait
* traiter les clés compromises
* révoquer des clés, y compris comment retirer ou désactiver des clés (clés compromises ou lorsqu'un utilisateur quitte l’organisation - les clés sont également archivées)
* récupérer les clés perdues ou corrompues
* sauvegarde ou archivage les clés
* détruire les clés
* enregistrer et auditer les activités liées à la gestion des clés
* définir les dates d'activation et de désactivation des clés
* traiter les demandes légales d'accès aux clés cryptographiques (mises à disposition d’informations cryptées sous une forme non cryptée comme preuve dans une affaire judiciaire)

Toutes les clés cryptographiques sont protégées contre la modification et la perte, cf. le fichier Clés cryptographiques. En plus les clés secrètes et privées sont protégées contre l'utilisation non autorisée ainsi que contre la divulgation. L'équipement utilisé pour générer, stocker et archiver les clés est physiquement protégé.

En plus de l'intégrité, pour de nombreux cas d'utilisation, l'authenticité des clés publiques est prise en compte.

L'authenticité des clés publiques est généralement traitée par des processus de gestion de clé publique utilisant des autorités de certification et des certificats de clé publique. Pour les clés à petit nombre, il est possible d’utiliser des technologies telles que l'application de processus manuels.

La cryptographie peut être utilisée pour atteindre différents objectifs de sécurité de l'information, comme :

* confidentialité : utilisation du cryptage des informations pour protéger les informations sensibles ou critiques, stockées ou transmises
* intégrité ou authenticité : utilisation de signatures numériques ou de codes d'authentification de message pour vérifier l'authenticité ou l'intégrité d'informations sensibles ou critiques stockées ou transmises. Utilisation d'algorithmes à des fins de vérification de l'intégrité des fichiers
* non-répudiation : utilisation de techniques cryptographiques pour apporter la preuve de l'apparition ou de la non-apparition d'un événement ou d'une action
* authentification : utilisation de techniques cryptographiques pour authentifier les utilisateurs et les autres entités du système demandant l'accès ou effectuant des transactions avec les utilisateurs, les entités et les ressources du système

La responsabilité de la gestion du chiffrement (quoi, comment, quand) est attribuée au RSI. Il peut demander des conseils de spécialistes externes.

Les solutions de chiffrement (Clés cryptographiques) sont définies et appliquées au niveau du réseau local et pour les transactions sensibles.

L’assurance d’intégrité et de non divulgation de ces clés est essentielle pour la sécurité du système de l’information.

Les perturbations électromagnétiques du transfert des informations sont qualifiées de signaux parasites. Leur interception permet de reconstituer les informations. Ces signaux deviennent alors des signaux parasites compromettants.

Le développement des systèmes sans fil montre l’apparition de signaux compromettants non parasites, nommés signaux compromettants intentionnels.

La protection contre les signaux compromettants est recommandée pour le traitement d’informations sensibles.

Le transfert de fichiers se fait via des sites FTP (*File Transfer Protocol* - protocole de transfert de fichier) sécurisés.

L’Interface web est sécurisée par le protocole SSL (*Secure Socket Layer* - couche de sécurisation des échanges) ou TLS (*Transport Layer Security* - sécurité de la couche de transport).

Des sanctions en cas de non-respect de la politique des mesures cryptographiques sont prévues, cf. le fichier Règles disciplinaires et le processus Appliquer la discipline.

La norme AES (*Advanced Encryption Standard* - norme de chiffrement avancé) est la plus utilisée comme algorithme de chiffrement symétrique.

Algorithmes de cryptage suggérés : AES128+, SHA512+, RSA2048+