Transfert de l’information

**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**

**5.1 Transfert de l’information**

**5.2 Transfert électronique**

**5.3 Transfert via un support de stockage physique**

**5.4 Transfert oral**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de maintenir la sécurité de l’information transférée au sein de l’organisation et avec toute partie intéressée externe.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Transfert de l’information » s’applique à l’ensemble du personnel réalisant le stockage, le transfert et le partage d'information afin de protéger celle-ci contre l’interception, la reproduction, la modification, les erreurs d’acheminement, le vol et la destruction.

**1.3 Glossaire**

SMSI – système de management de la sécurité de l’information

RSI – responsable sécurité de l’information

SI – 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**

Transfert de l’information

Classification de l’information

Accord fournisseur

Marquage

Traitement de l’information

Enregistrements

Propriété intellectuelle

Protection de la vie privée

Programmes malveillants

Contrôle d’accès

Utilisation de la cryptographie

Protection des supports lors du transport

Droits d’accès

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

A.5.14 Transfert de l’information

Des règles, des procédures ou des accords de transfert de l’information doivent être mises en place pour tous les types de transfert dans l’organisation et avec les autres parties.

**5. Déroulement**

**5.1 Transfert de l’information**

La politique Transfert de l’information est communiquée aux parties prenantes.

Les règles relatives au transfert de l’information sont conformes à la classification de l’information transférée selon la procédure Classification de l’information.

Tout transfert d’information avec des parties tierces est régit par des accords afin de protéger l’information, cf. Accord fournisseur.

Le transfert d’information est sous forme :

* électronique
* support de stockage physique
* verbal

Les règles générales de transfert d’information à respecter :

* utiliser des mesures de protection de l’information concernant l'interception, l'accès non autorisé, la copie, la modification, le mauvais acheminement, la destruction et le déni de service, y compris l'utilisation de la cryptographie
* utiliser des mesures concernant la traçabilité de l’information transférée
* identifier les propriétaires de l’information, les responsables du risque, les responsables de la sécurité
* notifier les personnes responsables en cas d'incidents de sécurité de l'information
* utiliser le système de marquage convenu pour les informations sensibles, cf. la procédure Marquage
* maîtriser la fiabilité et la disponibilité du service de transfert
* suivre les règles d'utilisation correcte et les procédures de traitement de l'information et des actifs selon la procédure Traitement de l’information
* conserver les enregistrements selon la procédure Enregistrements
* prendre en compte toute autre exigence légale, statutaire, réglementaire et contractuelle pertinente concernant la propriété intellectuelle et la vie privée selon les procédures Propriété intellectuelle et Protection de la vie privée

**5.2 Transfert électronique**

L’utilisation de la messagerie électronique (*courriel, email*) est considérée par défaut comme transfert d’information sensible. Restrictions :

* détection et protection contre les programmes malveillants selon la procédure Programmes malveillants
* protection d’information sensible dans un document attaché
* protection d’informations électroniques sensibles communiquées sous forme de pièce jointe
* prévention contre l'envoi de documents et de messages à la mauvaise adresse ou au mauvais numéro
* obtention d’une approbation avant d'utiliser des services publics externes (la messagerie instantanée, les réseaux sociaux, le partage de fichiers ou le stockage en nuage)
* utilisation de niveaux d'authentification plus élevés lors du transfert d'informations via des réseaux accessibles au public
* empêchement de transfert automatique de courrier électronique vers des adresses de courrier externes
* sensibilisation du personnel de ne pas envoyer de messages courts (SMS) ou de messages instantanés contenant des informations sensibles (ils peuvent être lus par des personnes non autorisées)
* sensibilisation du personnel sur les problèmes d'utilisation des télécopieurs (accès non autorisé aux messages, programmation délibérée ou accidentelle de machines pour envoyer des messages à des numéros spécifiques)
* en transmettant des informations à un collègue s’assurer qu’il est autorisé à les recevoir. Plus de détails dans la politique Contrôle d’accès
* le volume et la fréquence des transferts doivent être conformes au minimum requis
* restreindre l’envoi de documents en dehors de l’organisation et quand cela est fait demander l’autorisation de son chef direct
* tout fichier reçu est scanné pour des virus
* ne pas utiliser son courriel personnel au travail

Les réseaux sociaux présentent de nombreux avantages pour les organisations. Mais de nouveaux risques sont liés aux réseaux sociaux. Il est facile de nuire à la réputation d’une organisation, de se distraire et même de divulguer des informations sensibles.

Les données ou informations professionnelles et des commentaires déplacés sur les collègues ne doivent jamais être partagées sur des comptes de réseaux sociaux tels que Facebook, LinkedIn, etc.

Bénéfices possibles d’utilisation des réseaux sociaux :

* tirer parti des avantages commerciaux
* promouvoir ses produits/services
* contribuer à un dialogue pertinent en ligne
* mieux s'engager auprès des clients

Toute personne de l’organisation peut avoir besoin, à un moment donné, d'accéder à son travail depuis son domicile avec un ordinateur, un téléphone ou une tablette. Pour cela ne jamais utiliser des applications personnelles de stockage en nuage (*cloud*), comme iCloud, Google Drive, Box, Dropbox, Microsoft OneDrive, etc.

Utilisez le réseau « maison » avec authentification multi facteur. Pour plus de détails contactez le RSI.

Des techniques de cryptographie, par exemple pour protéger la confidentialité, l’intégrité et l’authenticité de l’information, sont utilisées dans notre organisation. Plus de détails dans la politique Utilisation de la cryptographie.

Quand les informations sont cryptées, elles sont protégées par un mot de passe fort et ne doivent jamais être copiées ou partagées d'une manière ou d’une autre.

Même si le cryptage des informations n’empêche pas dans l’absolu une violation des informations, il contribue à garantir que si des informations tombent entre de mauvaises mains, elles ne peuvent pas être lues ou utilisées.

**5.3 Transfert via un support de stockage physique**

Restrictions à prendre en compte lors du transfert utilisant des supports de stockage physique, y compris les documents papier :

* les responsabilités de contrôle et de notification de la transmission, de l'expédition et de la réception
* adressage et le transport corrects du message
* emballage protecteur (contre la chaleur, l'humidité les champs électromagnétiques) selon le document Protection des supports lors du transport
* coursiers fiables, standardisés, vérifiés et agréés par la direction
* selon le niveau de classification de l’information, utiliser des moyens de transport non altérables
* liste approuvée de prestataires de services de transport ou de messagerie en fonction de la classification de l’information
* tenue de journaux permettant d'identifier le contenu des supports de stockage, la protection appliquée ainsi que l'enregistrement de la liste des destinataires autorisés, les heures de transfert

Pour le stockage et le transfert d’information sur des dispositifs physiques, comme les clés USB, les cartes mémoire, les CD ou les disques durs externes, une validation est requise par le RSI. Les dispositifs sont fournis par l'organisation, ne pas utiliser de dispositifs venant de l’extérieur. Plus de détails dans la politique Droits d’accès.

N'utilisez JAMAIS ou ne branchez JAMAIS une clé USB que vous avez trouvée ou qui vous a été donnée comme article promotionnel. Ces dispositifs peuvent contenir des logiciels malveillants ou des virus cachés.

Un dispositif perdu ou volé doit être immédiatement signalé au département SI.

**5.4 Transfert oral**

L’ensemble du personnel est sensibilisé à ne pas tenir de conversation confidentielle dans des lieux publics, sur des réseaux de communication non sécurisés, dans des bureaux ouverts ou des lieux de réunion.

Pour protéger le transfert verbal d'informations, sensibiliser le personnel :

* ne pas avoir de conversations verbales confidentielles dans des lieux publics ou sur des canaux de communication non sécurisés
* ne pas laisser de messages contenant des informations confidentielles sur des répondeurs ou des messages vocaux
* filtrer au niveau approprié pour écouter une conversation
* s'assurer que les contrôles appropriés de la pièce sont appliqués (porte fermée,  insonorisation)
* commencer toute conversation sensible avec un avertissement afin que les personnes présentes connaissent le niveau de classification et les exigences de traitement de ce qu'elles sont sur le point d'entendre