Feuille informative

Points d'attention adressés aux communes en matière de sécurité de l'information

—

ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

EC 915

Traitement des données personnelles/sensibles

Accès au système d'information

- L'accès au système d'information doit être **personnel** et **individuel** (login + mot de passe).
- Limiter les accès aux **seules données (applications et fichiers) dont les utilisateurs (sociétés externes comprises) ont besoin** pour accomplir leurs tâches (selon le principe «need to know, need to do»).
- Établir une **matrice des droits d'accès** mentionnant quels utilisateurs possèdent quels accès (lire, muter, détruire, etc.) à quelles données, avec mention des noms des personnes ayant le pouvoir de modifier ces droits d'accès. Cette liste des droits d'accès devrait être mise à jour régulièrement.
- Les droits d'accès sont sous la responsabilité d'un ou de plusieurs responsables de traitement des données (qu'il faut définir).
- Mettre en place une **authentification forte** (nom + mot de passe + code) pour les accès aux applications sensibles effectués depuis l'extérieur de l'organisation.
- Ne pas laisser un prestataire externe accéder à distance à un ordinateur de l'organisation sans vérifier ce qui est réalisé et sans fermer les applications sensibles au préalable.

Transport de données

- Protéger les documents sensibles transportés en-dehors des locaux de l'organisation:
  - pour limiter les risques engendrés par le vol ou la perte de documents au format électronique, utiliser des **ordinateurs portables sécurisés avec des disques chiffrés;**
  - transporter les documents imprimés dans une **mallette sécurisée.**
- Ne jamais laisser de dossiers imprimés ou de matériel électronique professionnel dans un véhicule en stationnement et les ranger dans un lieu sûr lorsqu'il n'est pas possible de les ramener au bureau.
- **Chacun est responsable des informations qu'il emporte.**

Stockage des données

- Apporter un **niveau de protection élevé** à l'ensemble des données sensibles, quelles que soient leurs formes (dossiers imprimés, fichiers informatisés, etc.), le lieu et la durée de conservation.
- Ne pas laisser des **documents sensibles** sur les **imprimantes.**
- Les informations personnelles et confidentielles doivent être:
  - **mises sous clé,** protégées des regards externes et des risques de vol (dossiers imprimés);
  - **classées dans des dossiers (répertoires) protégés** au moyen de droits d'accès restreints aux seules personnes autorisées à les traiter.

Rectification des données

> Toute application informatique gérant des données personnelles devrait être construite sur un système de rectification des données permettant de tracer qui a modifié quoi, à quel moment, etc.
> Les données sensibles doivent être mises à jour régulièrement.

Sauvegarde des données

> S'assurer du **bon fonctionnement du système de sauvegarde** des données.
> **Numériser** le maximum de documents afin de garantir l'intégrité et l'intégralité des données.
> S'assurer que les **bases de données** contenant des données sensibles soient **chiffrées** ou que les moyens de protection de ces données soient adéquats.
> Stocker les bandes de sauvegarde dans des locaux sécurisés et dans des armoires qui ferment à clé.

Élimination des données

> A l'expiration du délai légal de conservation, les données sensibles doivent être éliminées de manière conventionnelle (**déchiqueteur à papier** ou **centrale d'incinération**).
> La destruction du matériel informatique et des imprimantes mis au rebut devraient être faite selon des procédures bien définies (**rayage des disques durs, mise hors service des smartphones,** etc.).

Traitement des données

> Tout traitement de données doit être licite et effectué conformément aux **principes de la bonne foi et de la proportionnalité.**
> Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances.
> La collecte des données personnelles doit être **reconnaissable** par la personne concernée.
> La manière dont chaque fichier est géré doit être définie **à toutes les étapes de son traitement** (création, traitement, communication, archivage, suppression, etc.).
> Un procédé **d'anonymisation** doit être utilisé aussi souvent que possible, lors d'échanges d'informations sensibles notamment.

Message électronique (e-mail)

—

› Éviter l'utilisation de l'e-mail **non chiffré** pour les communications de données officielles, personnelles ou sensibles.
› En dehors du réseau de l'Etat de Fribourg :
  • utiliser un système de chiffrement ;
    ou
  • protéger les documents transmis au moyen d'un **mot de passe fort** (remis par un autre canal de communication tel que le SMS ou le téléphone).
› Ne pas envoyer **d'information professionnelle** à une **adresse privée.**
› N'envoyer **aucune information sensible** à une **boite aux lettres électronique générique.**
› Avec l'e-mail, rester constamment centré sur l'identification de la demande et du demandeur, ainsi que sur la vérification du motif prépondérant.

Internet

—

› **Ne JAMAIS utiliser le mot de passe Windows ou celui d'une application métier sur Internet.**
› Certains logiciels permettant de transférer des fichiers par l'intermédiaire d'un navigateur Web (https://www.grosfichiers.com/ par exemple), utiliser des mots de passe forts pour chiffrer les fichiers transmis.
› **Attention:** les logiciels de transfert de fichiers n'entreposent généralement pas les fichiers en Suisse.

Téléphone

—

› **S'assurer de l'identité de l'interlocuteur** avant tout échange d'information.
› Transmettre des informations par téléphone **uniquement aux personnes ou aux organisations officielles en droit de les recevoir**:
  • rappeler le contact à son numéro officiel pour être certain de son identité;
    ou
  • poser les questions qui permettent de s'assurer de l'identité du contact.

Courrier

—

› S'assurer que les boîtes aux lettres de distribution du courrier (pelle de distribution, corbeille à courrier) ne soient pas accessibles à des personnes non autorisées.
› Définir les règles d'acheminement des courriers recommandés.

Appareils mobiles et supports amovibles

Appareils mobiles

- Sensibiliser à l'enregistrement et à la sauvegarde des données sensibles sur tout appareil mobile.
- Utiliser une application de gestion des appareils mobiles (MDM) pour gérer les données professionnelles à distance, surtout en cas de perte ou de vol.
- Imposer un mot de passe complexe sur tout appareil mobile (smartphone, tablette) utilisé à des fins professionnelles.
- Réglementer l'utilisation des appareils mobiles privés sur le lieu de travail.
- Chiffrer, autant que possible, les appareils mobiles (smartphone, tablette, ordinateur portable, etc.).

Supports amovibles

- Tenir un inventaire de tous les supports de données amovibles et en définir les règles d'utilisation.
- Si besoin, mettre à disposition des clés USB chiffrées pour un usage interne.
- Préconiser l'utilisation systématique du VPN pour accéder au système d'information depuis l'extérieure de l'organisation et sensibiliser sur les dangers du WIFI.

Collaborateurs

Arrivée d'un nouveau collaborateur

- Diffuser les directives de sécurité à chaque nouveau collaborateur.
- Informer les prestataires externes de la sensibilité des informations traitées.

Départ d'un collaborateur

- Supprimer les comptes des collaborateurs qui quittent l'organisation.
- **Désactiver les accès au système d'information et aux applications.**
- Supprimer les accès physiques aux bâtiments.
- **Modifier les éventuels mots de passe de groupe,** d'autant plus s'ils ont été créés pour des accès à des applications Web.

En cours d'activité

- **Mettre en place une sensibilisation régulière à la sécurité de l'information** pour toute personne qui accède au système d'information (collaborateurs, stagiaires, prestataires externes si nécessaire, etc.).
- Les thèmes abordés lors d'une telle sensibilisation sont très vastes. En voici quelques exemples:
  - gestion des mots de passe;
  - utilisation d'Internet;
  - utilisation des réseaux sociaux;
  - comportement face au «social engineering»;
  - comportement face à une usurpation d'identité;
  - utilisation de la messagerie électronique;
  - dangers de la mobilité, etc.
- **Remarque:** une bonne utilisation des logiciels métiers et bureautique a des conséquences autant sur l'efficacité du travail que sur la sécurité.

Accès aux locaux

- Equiper les locaux d'un système de détection d'incendie et/ou système de détection d'intrusion si des données sensibles sont stockées sous forme imprimée (archives ou autre).
- Fermer à clé les bureaux.
- Imposer aux collaborateurs le rangement de leur bureau en fin de journée ou lors des visites de clients.
- Chaque intervenant (interne ou externe) doit disposer d'un accès (physique) qui lui est propre.
- Ne pas laisser des externes seuls, accéder physiquement aux locaux qui contiennent des données sensibles.

Clause de confidentialité

- S'assurer qu'une **clause de confidentialité est conclue avec tous les prestataires externes** (dans le domaine informatique ou dans un autre domaine).

Poste de travail

- **Le verrouillage des postes de travail (ordinateurs et appareils mobiles) est la première protection contre l'intrusion.**
- Empêcher l'accès au système d'information, aux applications importantes et aux appareils mobiles après trois à cinq erreurs de connexion au maximum.
- **Enregistrer les fichiers sur les serveurs du réseau informatique** et non pas sur les ordinateurs de bureau ou sur les appareils mobiles.
- Installer un **outil d'enregistrement des mots de passe** pour une meilleure gestion des mots de passe par les utilisateurs.
- Mettre en place un système de connexion avec un mot de passe unique pour accéder à l'ensemble des applications métiers.
- Mettre en place **un système de contrôle des mots de passe** (complexes) pour respecter les bonnes pratiques en matière de sécurité.
- Ne pas permettre aux utilisateurs de modifier la configuration de leur ordinateur eux-mêmes, ni d'installer des logiciels.

Autorité cantonale de la transparence et de la protection des données ATPrD
Rue des Chanoines 2, CH-1700 Fribourg
T +41 26 322 50 08
-
www.fr.ch/atprd
-
Avril 2019
-
Source
Le contenu de ce document est une synthèse des points d'attention transmis aux communes ou autres administrations en matière de sécurité de l'information.