POLITIQUE DE SECURITE

OBJECTIFS

Pour améliorer la fiabilité des données, TFL veut tester une compagne de capteurs embarqués sur ses véhicules ils devraient leur permettre d’analyser les conditions d’un accident et/ou de le reproduire virtuellement, afin de faciliter les enquêtes sur la responsabilité des accidents.

En terme de sécurité, les données sont considérées comme sensible et doivent être sécurisées et cryptées, de leur collecte a leur traitement sans exception.

1 – Respecter une politique rigoureuse de mot de passe

En premier lieu, il faut adopter une politique rigoureuse de mot de passe, étant donné qu’il est le premier levier de sécurisation d’un poste informatique. La première des protections est donc de restreindre l’accès à un poste de travail ou à un fichier, via un identifiant et un mot de passe. Ce mot de passe doit impérativement être individuel, difficile à deviner et bien sûr demeurer confidentiel. En outre, il ne doit être inscrit sur aucun support. On doit déployer une politique de gestion des mots de passe particulièrement rigoureuse. Ainsi, un mot de passe devrait être constitué d’au moins 8 caractères, mêlant lettres, chiffres et caractères spéciaux. De même, il convient de le renouveler environ tous les trois mois, tout du moins de manière fréquente.

2 – Identifier de manière précise qui peut avoir accès aux données à protéger

L’accès aux fichiers regroupant les données personnelles doit être limité aux seules personnes qui en ont légitimement besoin dans l’exécution de leurs missions. Lors de chaque mouvement de salarié ou affectation d’un agent à un poste, le supérieur hiérarchique alors concerné doit identifier les fichiers auxquels ce dernier a besoin d’accéder, afin de lui en accorder les droits. Il doit également penser à faire la mise à jour de ces mêmes droits, régulièrement, afin d’en interdire l’accès aux salariés dont les activités ne le justifient plus.

3 – La sécurité réseaux :

Mettre en place une politique visant à sécuriser les infrastructures pour éviter que personne ne puisse accéder aux choses auxquelles il n'aurait pas accès, à une personne extérieure, éviter les attaques sur les serveurs, tout cela en coupant/partageant les portions de réseaux, mettre en place des firewall matériel et logiciel, mis en place de proxys, mise en place de filtre. etc...

4 – La sécurité système :

Pour la sécurité système il faut mettre en place une politique pour éviter qu'une personne accédant à une machine ne puisse modifier des fichiers systèmes, accéder à des informations dont il n'est pas propriétaires, déposer des virus, etc. Il faut mettre en place donc une politique de droits d'accès, de comptes utilisateurs/admin, des antivirus, des firewalls si besoin, des comptes de domaines, etc.

5 – La sécurité des données

5.1. Disponibilité, confidentialité et intégrité des données

Le traitement et le stockage des données numériques, l’accès aux applications et services et les échanges de données entre systèmes d’information doivent être réalisés selon des méthodes visant à prévenir la perte, la modification et la mauvaise utilisation des données ou la divulgation des données ayant un caractère sensible.

Une sauvegarde régulière des données avec des processus de restauration régulièrement validés doit être mise en place. On distinguera les sauvegardes de production (par exemple, restauration d’une donnée) des sauvegardes de recours (par exemple, reprise des services sur des moyens externes suite à incident majeur). Une étude fine des données (criticité, volatilité, fluctuation...) permettra de définir la périodicité et le type de sauvegarde ainsi que la durée de rétention dans le respect des législations en vigueur.

5.2. Protection des données sensibles

Le stockage et la transmission de données « classifiées de défense » sont interdits sauf utilisation de moyens spécifiques agréés au niveau national. L’habilitation en elle-même ne suffit pas pour accéder à un document classifié.

Les données non classifiées mais présentant un caractère sensible doivent être identifiées et le cas échéant repérées selon un niveau de sensibilité ; il sera procédé régulièrement à un réexamen de la sensibilité des données. Ces données devront faire l’objet d’une protection au niveau du contrôle d’accès (authentification et contrôle d’autorisation), du traitement, du stockage ou de l’échange (chiffrement) pour en assurer la confidentialité.

Avant toute cession ou mise au rebut d’un matériel ayant contenu des données sensibles, il est nécessaire de s’assurer que toutes les données ont bien été effacées par un procédé efficace et selon les recommandations techniques nationales. Si cela s’avère impossible les supports concernés devront être détruits.

5.3. Données à caractère personnel

Les traitements de données susceptibles de contenir des informations à caractère personnel (au sens de la loi n°78-17 du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés) doivent faire l’objet des formalités requises de déclaration ou de demande d’autorisation auprès de la CNIL, via la correspondant CIL de l’établissement.

Les données à caractère personnel constituent des données sensibles et comme telles doivent faire l’objet de protection.

5.4. Chiffrement

Le chiffrement, en tant que moyen de protection, est obligatoire pour le stockage et l’échange de données sensibles. Les produits matériels et logiciels utilisés doivent faire l’objet d’un agrément par la DCSSI. Une copie des clés permettant de restituer les données en clair doit être stockée dans un lieu externe et sécurisé.

AUTRES

================

Pour la sécurité des données, je pense que c'est pour le côté sauvegarde/sécurisation des données, d'où les logiciels de sauvegarde sur bandes, les disques RAID, les logiciels de sauvegarde sur disque.

L’hôpital doit restreindre l’accès aux données confidentielles et sensibles pour éviter qu’elles ne soient perdues ou compromises, de façon à ne pas nuire à nos clients, à ne pas encourir de sanctions pour non-conformité et à ne pas nuire à notre réputation. Parallèlement, nous devons faire en sorte que les utilisateurs puissent accéder aux données qui leur sont nécessaires pour travailler efficacement.

Il n’est pas attendu de cette politique qu’elle élimine tous les vols de données. Son principal objectif est plutôt de sensibiliser les utilisateurs et d’éviter les scénarios de perte accidentelle, c’est pourquoi elle décrit les exigences de prévention des fuites de données.

CHAMP D’APPLICATION

Dans le champ d’application

Cette politique s’applique à toutes les données définies comme sensible.

Elle s’applique donc à tous les serveurs, bases de données et systèmes informatiques qui traitent ces données, y compris aussi tout appareil utilisé pour le courrier électronique, l’accès au web ou autres tâches professionnelles.

Tout utilisateur interagissant avec les services informatiques de l’hôpital est également soumis à cette politique.

Hors du champ d’application.

Les informations classées comme publique ne sont pas soumises à cette politique.

Principes

L’hôpital fournira à tous ses employés et sous-traitants l’accès aux informations dont ils ont besoin pour leur travail.

Généralités

Chaque utilisateur doit être identifié par un ID user unique, afin que tous puissent être tenus pour responsables de leurs actions.

Dès lors l’utilisation des ID partagées n’est autorisée que là où elles sont appropriées. (Des comptes de formations par exemple)

Chaque utilisateur doit ratifier cette politique.

Les accès doivent être accordés selon le principe du moindre privilège, ce qui signifie que chaque programme et chaque utilisateur obtiendra seulement les privilèges qui lui sont nécessaires pour son travail.

Enregistré les accès des utilisateurs peuvent être utilisé comme éléments probants en cas d’enquêtes sur incident de sécurité.

Autorisation de contrôle d’accès

L’accès aux ressources et aux services informatiques de l’hôpital sera accordé par le biais d’un compte d’utilisateur unique et d’un mot de passe complexe (32 caractères, des MAJ, des chiffres et des caractères spéciaux).

Les mots de passe sont gérés par l’assistance informatique.

Responsabilités des utilisateurs.

Tous les utilisateurs doivent verrouiller leur écran chaque fois qu’ils quittent leur bureau, pour réduire le risque d’accès non autorisé.

Tous les utilisateurs doivent veiller à ne laisser aucune information sensible ou confidentielle autour de leur poste de travail.

Tous les utilisateurs doivent tenir leurs mots de passe confidentiels et ne pas les partager.

Accès aux applications et aux informations.

Tous les employés et sous-traitants de l’hôpital doivent bénéficier d’un accès aux données et aux applications nécessaires à leur fonction professionnelle.

Tous les employés et sous-traitants ne doivent accéder aux données et systèmes sensibles qu’en cas de nécessité professionnelle et avec l’accord de la direction.

Les systèmes sensibles doivent être physiquement ou logiquement isolés afin d’en restreindre l’accès au personnel autorisé uniquement.

Accès aux réseaux

Un accès aux réseaux doit être accordé à tous les employés et sous-traitants, selon les procédures de contrôle d’accès de l’entreprise et le principe du moindre privilège.

Tous les employés et sous-traitants bénéficiant d’un accès distant aux réseaux de l’entreprise doivent être authentifiés par le mécanisme d’authentification du VPN uniquement.

Les réseaux doivent être séparés selon les recommandations issues des recherches de sécurité sur les réseaux de l’entreprise. Les administrateurs réseaux doivent regrouper les services et systèmes informatiques et les utilisateurs selon les besoins de cette séparation.

Des contrôles de routage des réseaux doivent être mis en place pour appliquer la politique de contrôle d’accès.

Accès aux informations confidentielles et restreintes

L’accès aux données classées comme « confidentielles » ou « restreintes » doit être limité aux personnes autorisées dont les responsabilités professionnelles l’exigent, tel que déterminé par la Politique de sécurité des données ou la direction.

Le service de sécurité informatique est responsable d’instaurer les restrictions d’accès.