
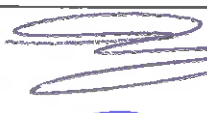


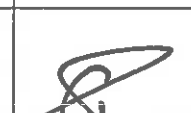


POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION DU CENTRE HOSPITALIER SUD GIRONDE

	Rédaction	Vérification	Validation	Approbation	Date
Noms	J.P. COUTANT Réfèrent sécurité Informatique	L. BESSE Responsable Informatique F. CRESPO-GARCIA Directrice Adjointe	Pour le comité de piloteage, F. BELLOUGUET Directrice des soins, de la qualité et de la gestion des risques	F. CRESPO-GARCIA Directeur délégué	d'application : 30 AVR. 2018 Date de la prochaine remise à jour : 30 AVR. 2021 Remise à jour faite : Oui Non
Signatures		 			
Date	03/04/18	11/04/18	26/04/18	27/04/18	

REFERENCE :

Le présent document est rédigé selon les recommandations des différentes autorités compétentes dans le domaine de la sécurisation des systèmes d'information (ASIP, CERTA, CNIL, ...).

Il est une déclinaison de la PSSE (Politique de sécurité des systèmes d'information de l'Etat) et de la PSSI-MCAS et de la (Politique de sécurité des systèmes d'information pour les Ministères chargés des affaires sociales) auxquelles les établissements de santé doivent se conformer.

DEFINITION :

La sécurité des systèmes d'information ne repose pas exclusivement sur des outils, elle repose aussi sur une organisation et des politiques.

a) Le processus de prise en charge du patient au cœur du système

Le métier de l'hôpital impose de placer le patient au cœur de la politique de sécurité :

- rechercher en permanence un compromis acceptable entre impératifs d'efficacité du soin et impératifs de sécurité de l'information ;
- respecter le droit à la vie privée du patient par la garantie de l'anonymat et à l'assurance de la confidentialité des informations médicales.

b) Les processus support concernés par la sécurité du système d'information

La politique de sécurité s'applique également aux informations concernant le personnel et les fournisseurs.

La sécurité de l'information est caractérisée comme étant la préservation de :

- sa **confidentialité** : faire en sorte que l'information ne soit accessible qu'aux personnes autorisées à y accéder ;
- son **intégrité** : protéger l'exactitude et l'intégrité de l'information et des méthodes de traitement
- sa **disponibilité** : faire en sorte que les utilisateurs autorisés puissent accéder à l'information lorsqu'ils en ont besoin ;
- les **moyens de preuves** et contrôles nécessaires aux utilisateurs pour accorder leur confiance dans l'information fournie.

OBJECTIFS :

Ce document a pour objectif de définir les modalités de sécurisation du système d'information de l'établissement.

DOMAINE D'APPLICATION :

La politique de sécurité de l'information a pour objet la protection de toute information, gérée par le système d'information automatisé et échangée ou non avec l'extérieur.

La Politique de Sécurité des Systèmes d'Information du Centre Hospitalier décrite dans ce document est constituée de l'ensemble, formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'établissement.

Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'établissement à la sécurité de son système d'information.

ABREVIATIONS :

ASIP : Agence des Systèmes d'Information Partagés

CERTA : Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques

CNIL : Commission Nationale de l'Informatique et des Libertés

CPS : Carte de Professionnel de Santé

DRH : Direction des Ressources Humaines

SIH : Système d'Information Hospitalier

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

DESTINATAIRES :

Ce document est à destination de l'ensemble des utilisateurs du système d'information de l'établissement.

HISTORIQUE DES MODIFICATIONS :

<i>Indice</i>	<i>Date</i>	<i>Nature de la modification</i>	<i>Page</i>
A	17/09/2012	Création	
B	02/12/2015	Mise à jour	5
C	21/07/2017 20/04/18	A propos de la charte Accès distant au SIH	5

Table des matières

1	Organisation – Gouvernance	5
1.1	Gouvernance	5
1.2	Référent de la sécurité du Système d'Information	5
2	Ressources humaines	5
2.1	Utilisateurs autorisés à accéder au SIH	5
2.2	Les chartes d'accès au SIH des utilisateurs	5
3	Exploitation des accès	6
3.1	Attribution des accès et gestion des mouvements de personnel	6
3.2	Gestion des mots de passe	6
3.3	Carte CPS	6
4	Administrateurs du SI	6
4.1	Charte des administrateurs des ressources informatiques	6
4.2	Traçabilité des interventions sur le système	7
4.3	Gestion des identifiants « administrateurs » du service informatique	7
a)	Accès aux outils d'administration	7
b)	Séquestre des identifiants	7
c)	Politique de mots de passe « administrateurs »	7
d)	Gestion du départ d'un administrateur des SI	7
e)	Gestion des actions d'administration	7
f)	Nomenclature des comptes du domaine	7
g)	Restreindre au maximum l'appartenance aux groupes d'administration du domaine	7
4.4	Prise de main à distance	7
4.5	Sécurisation des flux d'administration	8
4.6	Formations et sensibilisation des utilisateurs	8
5	Exploitation technique	8
5.1	Configuration des ressources informatiques	8
5.2	Configuration du navigateur Internet	8
5.3	Mise à jour des systèmes et des logiciels	8
a)	Application des correctifs de sécurité	8
b)	Déploiement des correctifs de sécurité	8
c)	Assurer la migration des systèmes obsolètes	9
d)	Isoler les systèmes obsolètes restants	9
6	Gestion des biens	9
6.1	Inventaire des ressources informatiques	9
6.2	Mise au rebut	9
7	Gestion des prestataires	9
8	Sécurité des réseaux locaux	9
8.1	Elaborer les documents d'architecture technique et fonctionnelle	9
8.2	Accès aux réseaux	9
9	Sécurité des postes de travail	10
a)	Fourniture et gestion des postes de travail	10
b)	Formalisation de la configuration des postes de travail	10
c)	Réaffectation du poste de travail	10
d)	Privilèges des utilisateurs sur les postes de travail	10
e)	Utilisation des privilèges d'accès « administrateur »	10
f)	Gestion du compte « administrateur local »	10
g)	Stockage des informations	10
h)	Partage de fichiers	10

i)	Suppression des données sur les postes partagés	11
j)	Fourniture de supports de stockage amovibles.....	11
k)	Maîtrise des matériels.....	11
l)	Déclarer les pertes et vols.....	11
m)	Données enregistrées sur les postes de travail et dans les messageries par les utilisateurs	11
n)	Sauvegarde des données utilisateurs	11
10	Traitement des alertes de sécurité émises par les instances nationales ou régionales (FSSI / ANSSI / ARS).....	11
a)	Mobilisation en cas d'alerte.	11
b)	Remontée des incidents.	12
11	Continuité d'activité.....	12
11.1	Mise en œuvre des dispositifs techniques et des procédures opérationnelles	12
11.2	Exercice régulier du plan de reprise d'activité du système d'information	12
11.3	Mise à jour du plan de reprise d'activité du système d'information	12
12	Lutte contre les codes malveillants	12
12.1	Protection contre les codes malveillants	12
12.2	Gestion des événements de sécurité de l'antivirus	12
12.3	Mise à jour de la base de signatures.....	12
12.4	Filtrage URL et Pare feu	12
12.5	Anti-spam – Filtrage des messages électroniques.....	12
13	Sécurité physique des locaux	13
13.1	Alimentation électrique.....	13
13.2	Accès aux salles de serveurs	13
13.3	Climatisation	13
13.4	Lutte contre l'incendie	13

1 Organisation – Gouvernance

1.1 Gouvernance

La politique de sécurité du système d'information est rédigée par la Direction Informatique et présentée au comité de suivi et aux instances (à définir). Elle est validée par la Direction du Centre Hospitalier. Elle est mise en œuvre par le service informatique et le service biomédical dans leur domaine de compétence respectif.

1.2 Référent de la sécurité du Système d'Information

Le Référent Sécurité du Système d'Information est un personnel du service informatique. Il est clairement identifié et ses fonctions sont indiquées dans sa fiche de poste.

L'équipe informatique de l'établissement préconise des règles, des outils, des bonnes pratiques à appliquer.

2 Ressources humaines

La règle de base appliquée systématiquement par l'établissement est la suivante :

Tous les accès au SIH des utilisateurs qui n'ont pas été explicitement autorisés sont bloqués. Pour être acceptés, ces accès doivent pouvoir être auditables et suivre les normes, lois et règles en vigueur ainsi que les préconisations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

2.1 Utilisateurs autorisés à accéder au SIH

Les utilisateurs peuvent être des personnels permanents, des professionnels de santé libéraux, des professionnels de santé d'autres structures hospitalières, des professionnels de santé intérimaires, des étudiants, des personnels de structures de recherche autorisés par le Directeur du Centre Hospitalier, des prestataires du service informatique, du service biomédical ou du service techniques.

2.2 Les chartes d'accès au SIH des utilisateurs

Une charte d'accès au SIH (ADM/SIH/ENG 001.1B) est remise à toutes les personnes recrutées par le Centre Hospitalier avant son embauche. Elle est implicitement acceptée, opposable et intégrée au règlement intérieur.

Les utilisateurs sont informés des mises à jour (nouvelles versions) apportées à la charte d'accès au système d'information par une pièce jointe au bulletin de salaire.

Une charte d'accès au SIH (ADM/SIH/ENG 001.4) est remise à toutes les personnes qui n'appartiennent pas à l'entité et dont l'activité nécessite l'accès au SIH. Elle est signée et transmise au service informatique avant la remise des identifiants de connexion.

Une charte d'accès distant au SIH (ADM/SIH/ENG 001.6A et ADM/SIH/ENG 001.3A) est également remise aux personnes autorisées par le Directeur du Centre Hospitalier à se connecter au SIH depuis l'extérieur du Centre Hospitalier. Elle est signée et transmise au service informatique avant la remise des identifiants de connexion.

Une charte d'utilisation d'Internet (ADM/SIH/ENG 001.2A) est remise à toutes les personnes qui n'appartiennent pas à l'entité et qui bénéficie d'un accès à internet. Elle est signée et transmise au service informatique avant ouverture de l'accès.

Les chartes d'accès au SIH sont intégrées au système de gestion documentaire de l'établissement et font donc l'objet d'une codification attribuée par le gestionnaire documentaire. Elles sont également disponibles sur le portail Intranet du Centre Hospitalier.

3 Exploitation des accès

3.1 Attribution des accès et gestion des mouvements de personnel

Les droits définis sur les postes de travail et dans les applications sont limités. Ils sont attribués en fonction des besoins de chaque utilisateur pour l'exercice de leurs fonctions.

Une procédure (ADM/SIH/PRC 017A) décrit la gestion des utilisateurs du système d'information. Une procédure (ADM/SIH/PRC 019A) décrit les accès aux données médicales.

3.2 Gestion des mots de passe

L'accès au système d'information se fait grâce à une signature électronique individuelle constituée d'un code utilisateur et d'un mot de passe.

L'utilisateur ne doit jamais divulguer sa signature à d'autres utilisateurs.

La politique de gestion des mots de passe est conçue de façon à protéger contre les attaques par essais successifs de mots de passe. Une complexité minimale dans le choix des mots de passe est imposée aux utilisateurs.

La validité du mot de passe est limitée dans le temps.

Une procédure (ADM/SIH/PRC 027) décrit la gestion des mots de passe du système d'information.

3.3 Carte CPS

Le personnel des admissions, de la facturation, des urgences et de la surveillance continue sont dotées de cartes CPS afin de pouvoir visualiser les droits des assurés. Elles permettent également de se connecter au système d'information aux urgences et en surveillance continue ainsi qu'au système de télé-thrombolyse.

4 Administrateurs du SI

4.1 Charte des administrateurs des ressources informatiques

Une charte des administrateurs SI et biomédicaux (ADM/SIH/DOC 029) est remise à toutes les personnes du Centre Hospitalier en charge de l'administration d'une ressource. Elle est implicitement acceptée et opposable.

4.2 Traçabilité des interventions sur le système

Les interventions de maintenance sur les ressources informatiques de l'entité sont tracées par le service informatique.

Les interventions de maintenance sur les ressources biomédicales de l'entité sont tracées par le service biomédical.

4.3 Gestion des identifiants « administrateurs » du service informatique

a) Accès aux outils d'administration.

L'accès aux outils et interfaces d'administration est strictement limité aux personnes habilitées.

b) Séquestre des identifiants

Les comptes utilisateurs permettant l'administration des ressources des SI sont placés sous séquestre et tenus à jour, dans un logiciel et un coffre ignifugé fermé à clé.

c) Politique de mots de passe « administrateurs »

Chaque administrateur dispose de mots de passe propres et destinés à l'administration.

d) Gestion du départ d'un administrateur des SI

En cas de départ d'un administrateur disposant de privilèges sur des composants du système d'information, les comptes individuels dont il disposait sont immédiatement désactivés. Les éventuels mots de passe d'administration dont il avait connaissance sont changés (exemples : mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur).

e) Gestion des actions d'administration.

Les opérations d'administration sont tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration.

f) Nomenclature des comptes du domaine.

La gestion des comptes doit s'appuyer sur une nomenclature adaptée, afin de pouvoir distinguer selon leur usage : comptes d'utilisateur standard, comptes d'administration (domaine, serveurs, postes de travail) et comptes de service.

g) Restreindre au maximum l'appartenance aux groupes d'administration du domaine.

L'appartenance aux groupes du domaine ADMINISTRATEURS et ADMINISTRATEURS DU DOMAINE n'est nécessaire que dans de très rares cas. Les opérations les plus courantes doivent être effectuées avec des comptes du domaine membres des groupes locaux d'administration des ordinateurs ou ayant une délégation d'administration.

4.4 Prise de main à distance

La prise de main à distance d'une ressource informatique ou biomédicale n'est réalisable que par les personnels autorisés par l'équipe locale chargée du système d'information, sur les ressources informatiques de leur périmètre.

4.5 Sécurisation des flux d'administration.

Les opérations d'administration sur les ressources locales d'une entité doivent s'appuyer sur des protocoles sécurisés.

4.6 Formations et sensibilisation des utilisateurs

Elles concernent les utilisateurs référents et l'équipe informatique.

Des actions de sensibilisation et de formation à la sécurité ont été mises en place.

Chacun doit être conscient des risques liés à la diffusion d'informations médicales ou personnelles dans un système ouvert à l'extérieur.

Pour faire face aux risques, le service informatique doit maintenir un niveau élevé et actualisé de ses connaissances dans le domaine de la sécurité informatique par :

- des formations,
- de la veille technique,
- des échanges avec les services informatiques des autres hôpitaux.

Le service informatique suit les préconisations de l'ANSSI diffusées par l'intermédiaire d'internet, de messageries et de formations.

5 Exploitation technique

5.1 Configuration des ressources informatiques

Les systèmes d'exploitation et les logiciels doivent faire l'objet d'un durcissement. Les configurations et mises à jour sont appliquées dans le strict respect des guides ou procédures en vigueur.

5.2 Configuration du navigateur Internet.

Le navigateur déployé par l'équipe locale chargée du système d'information sur l'ensemble des serveurs et des postes de travail nécessitant un accès Internet ou Intranet doit être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).

5.3 Mise à jour des systèmes et des logiciels

a) Application des correctifs de sécurité

Le maintien dans le temps du niveau de sécurité d'un système d'information impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à chaque système ou applicatif est défini, et adapté suivant les contraintes et le niveau d'exposition du système.

b) Déploiement des correctifs de sécurité

Les correctifs de sécurité des ressources informatiques locales doivent être déployés par l'équipe informatique.

c) Assurer la migration des systèmes obsolètes

L'ensemble des logiciels utilisés sur le système d'information doit être dans une version pour laquelle l'éditeur assure le support, et tenu à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.

d) Isoler les systèmes obsolètes restants.

Il est nécessaire d'isoler les systèmes obsolètes, gardés volontairement pour assurer un maintien en condition opérationnelle des fonctionnalités, et pour lesquels une migration n'est pas envisageable. Chaque fois que cela est possible, cette isolation doit être effectuée au niveau du réseau (filtrage strict), des éléments d'authentification (qui ne doivent pas être communs avec le reste du SI) et des applications (pas de ressources partagées avec le reste du SI).

6 Gestion des biens

6.1 Inventaire des ressources informatiques

Le service informatique et le service biomédical établissent et maintiennent à jour leur inventaire des ressources informatiques sous leur responsabilité, en s'appuyant sur un outillage adapté. Il comprend la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes. Il est constitué d'une base de données de configuration, maintenue à jour. L'historique des attributions des biens inventoriés est conservé, dans le respect de la législation.

6.2 Mise au rebut

Lorsqu'une ressource informatique ou biomédicale est amenée à quitter définitivement l'entité, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée ou le support d'information détruit.

7 Gestion des prestataires

Une charte d'accès au SIH « Fournisseurs et prestataires » (ADM/SIH/DOC 031) est remise au représentant du fournisseur qui la signe.

8 Sécurité des réseaux locaux

8.1 Elaborer les documents d'architecture technique et fonctionnelle.

L'architecture réseau du système d'information est décrite et formalisée à travers des schémas d'architecture, et des configurations, maintenus au fil des évolutions apportées au SI. Les documents d'architecture sont sensibles et font l'objet d'une protection adaptée.

8.2 Accès aux réseaux.

Le contrôle physique des accès réseaux, l'attribution des adresses IP, le filtrage des informations et l'usage de dispositifs spécifiques (machines virtuelles, cartes d'administration à distance, etc.) font l'objet de procédures sécurisées.

Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'une entité.

Dans le cas où le Centre Hospitalier partage des locaux (bureaux ou locaux techniques) avec des entités externes, des mesures de cloisonnement des ressources informatiques sont mises en place (GCS Imagerie, autres Centre Hospitaliers).

9 Sécurité des postes de travail

a) Fourniture et gestion des postes de travail.

Les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par l'équipe informatique.

Si un poste est mis à disposition par une autre voie, sa connexion au réseau est soumise à l'autorisation du référent informatique.

b) Formalisation de la configuration des postes de travail.

Une procédure formalisée de configuration des postes de travail est établie par le service informatique et conservée dans son système documentaire (FPE-Mode opératoire Poste de Travail).

c) Réaffectation du poste de travail.

Une procédure définie les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés. Elle est conservée dans le système documentaire du service informatique (FPE-Mode opératoire réaffectation des postes de travail).

d) Privileges des utilisateurs sur les postes de travail.

La gestion des privilèges des utilisateurs sur leurs postes de travail suit le principe du « moindre privilège » : chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission.

e) Utilisation des privilèges d'accès « administrateur »

Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.

f) Gestion du compte « administrateur local »

L'accès au compte « administrateur local » sur les postes de travail doit être strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail.

g) Stockage des informations

Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés.

Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de sauvegarde sont en place.

h) Partage de fichiers

Le partage de répertoires ou de données hébergées localement sur les postes de travail est pros crit.

i) Suppression des données sur les postes partagés

Les données présentes sur les postes partagés (portable de prêt, par exemple) doivent être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître.

j) Fourniture de supports de stockage amovibles

Les supports de stockage amovibles (clés USB et disque durs externes, notamment) doivent être fournis aux utilisateurs par le service informatique et sont les seuls à pouvoir être connectés aux postes de travail.

k) Maîtrise des matériels.

Les postes de travail - y compris dans le cas d'une location - sont fournis à l'utilisateur par l'entité, gérés et configurés sous la responsabilité du service informatique. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'entité (qu'il s'agisse de téléphones connectés, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur des équipements et des réseaux professionnels est interdite.

l) Déclarer les pertes et vols.

Toute perte ou vol d'une ressource d'un système d'information doit être déclarée au référent sécurité et à la CNIL par l'établissement.

m) Données enregistrées sur les postes de travail et dans les messageries par les utilisateurs

Les données enregistrées sur les matériels de l'hôpital sont des données professionnelles. A moins qu'elles n'aient été clairement identifiées comme des données strictement personnelles par l'utilisateur, elles peuvent être accessibles par la direction du Centre Hospitalier si nécessaire. Le service informatique peut également y accéder si des opérations de maintenance indispensables doivent être réalisées (cas de la présence de virus par exemple).

Les utilisateurs doivent respecter les règles de la propriété intellectuelle.

n) Sauvegarde des données utilisateurs

Les données des utilisateurs enregistrées dans le répertoire « Mes documents » des postes de travail ainsi que sur le bureau sont sauvegardées sur une baie de stockage dédiée. Les éléments sont ainsi conservés pendant trois semaines glissantes. Tout fichier de type média audio, vidéo ou image est exclu de cette sauvegarde. Ces répertoires « Mes documents » et « Bureau » ne sont pas considérés comme des répertoires de données strictement personnelles.

Les fichiers type archive de messagerie sont également sauvegardés selon le même procédé.

10 **Traitement des alertes de sécurité émises par les instances nationales ou régionales (FSSI / ANSSI / ARS)**

a) Mobilisation en cas d'alerte.

En cas d'alerte de sécurité identifiée au niveau national, le référent sécurité s'assure de la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.

b) Remontée des incidents.

Les incidents de sécurité sont traités en suivant la fiche réflexe ADM/SIH/PRT 026.

11 Continuité d'activité

11.1 Mise en œuvre des dispositifs techniques et des procédures opérationnelles

Les équipes informatiques mettent en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la continuité du système d'information, en assurent la supervision au quotidien et la maintenance dans le temps.

11.2 Exercice régulier du plan de reprise d'activité du système d'information

Le référent sécurité et le responsable informatique organise des exercices réguliers, afin de tester le plan de reprise d'activité de système d'information.

11.3 Mise à jour du plan de reprise d'activité du système d'information

Le référent sécurité et le responsable informatique assure le maintien à jour du plan de reprise d'activité (ADM/SIH/DOC 016A) du système d'information.

12 Lutte contre les codes malveillants

12.1 Protection contre les codes malveillants

Des logiciels de protection contre les codes malveillants, appelés communément antivirus, doivent être installés sur l'ensemble des serveurs et des postes de travail de l'entité.

12.2 Gestion des événements de sécurité de l'antivirus

Les événements de sécurité de l'antivirus sont analysés (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

12.3 Mise à jour de la base de signatures

Les mises à jour des bases antivirales et des moteurs d'antivirus sont déployées automatiquement sur les serveurs et les postes de travail.

12.4 Filtrage URL et Pare feu

Le filtrage URL consiste à bloquer l'accès à des sites internet potentiellement ou réellement dangereux. L'administration de ces outils est réalisée par un prestataire. Le filtrage peut être complété par le service informatique de l'établissement mais celui-ci n'a accès à la configuration des règles de sécurité qu'en consultation.

12.5 Anti-spam – Filtrage des messages électroniques

Cette prestation est réalisée par l'hébergeur de la messagerie électronique. Les messages contenant des pièces jointes potentiellement dangereuses sont bloqués. Les messages de type « SPAM » sont marqués comme étant des messages indésirables et chaque utilisateur peut les filtrer automatiquement avec son outil de messagerie.

13 Sécurité physique des locaux

13.1 Alimentation électrique

L'alimentation électrique des équipements doit être conforme aux règles de l'art, de façon à se prémunir des atteintes à la sécurité des personnes et équipements liées à un défaut électrique.

13.2 Accès aux salles de serveurs

L'accès aux salles hébergeant les serveurs est réservé aux personnes chargées des sauvegardes et de l'exploitation informatique, aux services techniques dans le cadre d'interventions de maintenance, aux personnes chargées de la sécurité et aux prestataires de maintenance accompagnés. L'accès à la salle principale est tracé.

13.3 Climatisation

Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique est installé. Des procédures de réaction en cas de panne, connues du personnel, sont élaborées et vérifiées annuellement.

13.4 Lutte contre l'incendie

Les salles informatiques sont équipées d'une détection incendie avec des détecteurs de fumées. En cas de problème, la détection incendie assure un report d'alarme vers le standard et le service des urgences. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu ne doit être entreposé dans ces locaux.

Le système de détection bénéficie d'un contrat de maintenance 7j/7j.

