PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé

Sommaire

1 Préambule

La charte sécurité du S.I., annexe du Règlement Intérieur de l'hôpital, est entrée en application en novembre 2020. Elle a fait l'objet d'une consultation des instances représentatives du personnel et est opposable.
Elle a pour objectifs d'informer le personnel sur ses droits, ses obligations et ses responsabilités en matière de sécurité de l'information. Les personnels de la DSN, en tant que membres du personnel hospitalier, sont soumis au respect de cette charte.
Pour autant, la nature de leur mission leur confère un rôle particulier par rapport au Système d'Information. Le présent document précise donc les droits et obligations de ces personnels en complément de ceux mentionnés dans la charte informatique et règlement intérieur.

2 Domaine d'application

Le présent document est applicable à l'ensemble des personnels de la DSN, quel que soit leur statut (salariés et non-salariés, stagiaires, personnel intérimaire), ainsi qu'aux personnels extérieurs exerçant une mission au sein de la DSN (consultants, sous-traitants, fournisseurs, formateurs, …). Les responsables, côté DSN, de ces utilisateurs externes s'engagent à faire respecter la présente charte par toute personne placée sous leur responsabilité.
Dans la suite de ce document, on distinguera 3 catégories de comptes à la DSN :

- **Nominatif** **compte utilisateur sans droit administrateur du PC**
- **Administrateur** **compte pour administrer les serveurs CHU**
- **Admin GHT HDS** **compte pour administrer les serveurs GHT et HDS**

Le Directeur et son adjoint sont soumis à l'ensemble des obligations sécurité.
Le secrétariat est soumis aux mêmes obligations sécurité.

3 Objectifs

De par leurs fonctions, les personnels de la DSN sont chargés notamment d'assurer le bon fonctionnement du Système d'Information et de protéger le patrimoine informationnel de l'hôpital, et ce, dans le respect de la réglementation et des procédures internes en vigueur.
Dans ce cadre, l'hôpital a accordé à ces personnels le droit d'accéder aux données et ressources matérielles et logicielles nécessaires. Un tel accès n'est contraire à aucune disposition légale car il est dans les attributions de ces personnels d'y avoir accès pour développer, maintenir ou administrer les systèmes, ou éviter les malveillances, abus et dysfonctionnements.
De ce fait, les personnels de la DSN s'engagent dans la durée de leur contrat ainsi qu'après sa cessation, à observer la discrétion la plus absolue sur les informations de toute nature, notamment personnelles et/ou confidentielles, auxquelles ils pourraient avoir accès, et à ne jamais les divulguer ou en favoriser la divulgation, en dehors de leur mission.
En tant que garants du bon fonctionnement et de la bonne utilisation des moyens informatiques et de communication, l'hôpital attend de leur part une attitude exemplaire quant à l'utilisation de ces accès.
Le non-respect de cette charte peut entraîner une action disciplinaire et/ou judiciaire proportionnelle à la gravité des faits.

4 Liste des obligations

N°		Users	Adm CHU	Adm GHT HDS
4.1 Politique de Sécurité				
1	Le personnel-DSN doit respecter la Politique de Sécurité du Système d'Information (PSSI) et les chartes sécurité en vigueur dans la structure. Il doit respecter, en tant qu'utilisateur du système, les règles qu'il est amené à imposer ou qui sont imposées aux autres utilisateurs.	*	*	*
4.2 Comptes informatiques et mots de passe				
2	Le personnel-DSN dispose de trois types de compte : un compte « standard », ayant des droits standard sur son ordinateur. Et un compte dit « administrateur » ayant des droits supplémentaires. Et un compte administrateur GHT et HDS En règle générale, il faut utiliser le compte standard. Notamment pour la connexion sur le poste d'un utilisateur. Les comptes « administrateurs » ne doivent être utilisés qu'à partir des postes d'administration et lorsque le compte standard est insuffisant.	*	*	*
3	Tous les travaux d'administration (tels que des tâches planifiées, ou des programmes automatiques de transfert de données) ainsi que les permissions fichiers associées doivent être réalisés avec des comptes spécifiques dédiés (ou des groupes de comptes pour les permissions) et non avec des comptes personnels, y compris à des fins de tests. Si le mot de passe d'un personnel-DSN devait être réinitialisé sans préavis par la direction du service, cela ne devrait entraîner aucune conséquence sur le bon fonctionnement des systèmes.	*	*	*
4	Le personnel-DSN doit s'assurer que tous les comptes et mots de passe de services qu'il utilise pour l'administration des différents systèmes soient dûment documentés et enregistrés dans un référentiel de mots de passe, défini et accessible à tout moment par la Direction du service et par les personnels-DSN autorisés : Teampass avec les comptes de services. Le mot de passe d'accès à ce référentiel est hautement sensible. Il doit être mémorisé par les personnes habilitées à accéder au référentiel, et ressaisi à chaque accès. En aucun cas, il ne doit être inscrit sur un papier ou dans un fichier, quelle que soit la sécurité associée à ce fichier.		*	*
5	Le personnel-DSN doit utiliser des mots de passe personnels robustes : mélange de lettres, chiffres et caractères spéciaux, longueur minimum de 12 caractères pour leur compte utilisateur et 15 caractères pour leurs comptes administrateurs. Ils doivent être changés au moins tous les 6 mois. Ils sont strictement personnels et ne doivent jamais être divulgués, à l'intérieur comme à l'extérieur de la DSN. En aucun cas, ces mots de passe ne doivent être inscrits sur un papier ou dans un fichier, quelle que soit la sécurité associée à ce fichier.	*	*	*
6	Les mots de passe utilisés dans les différents systèmes ou dans des programmes doivent être robustes au même titre que les mots de passe personnels. Ils doivent être propres à chaque système ou groupe de systèmes, dans certains cas. La portée de chaque mot de passe doit ainsi être limitée : les mots de passe administrateur locaux de chaque serveur et poste sont différents. Lorsque des prestataires installent ou interviennent sur un système, le personnel-DSN qui suit la prestation doit veiller à faire appliquer ce niveau de robustesse aux mots de passe positionnés par le prestataire.	*	*	*
7	Le personnel-DSN n'a pas besoin de connaître les mots de passe des utilisateurs pour mener à bien sa mission, et ne doit donc jamais demander à un utilisateur la communication de son mot de passe. Il doit expliquer ce principe de façon claire aux utilisateurs et le leur rappeler si nécessaire. Ainsi, si une authentification d'un utilisateur est nécessaire, il invitera l'utilisateur à saisir son mot de passe. Lorsque des utilisateurs communiquent tout de même leur mot de passe	*	*	*

N°		Users	Adm CHU	Adm GHT HDS
	(mauvaise information de l'utilisateur ou cas d'urgence), le personnel-DSN doit ensuite inviter l'utilisateur à le changer en lui indiquant la marche à suivre.			
8	Lors de l'arrivée d'un nouveau salarié, la remise de ses comptes et mots de passe doit respecter la procédure en vigueur de remise des comptes. Celle-ci prévoit notamment une formation permettant à l'utilisateur de changer immédiatement ses mots de passe initiaux, ainsi qu'une invitation à signer la bonne réception de ses comptes assortie d'un engagement de confidentialité.	*	*	*
9	Lors de la réinitialisation d'un mot de passe perdu/oublié/compromis, la personne qui fait la réinitialisation et qui communique le nouveau mot de passe doit s'assurer de l'identité de l'interlocuteur auquel le mot de passe est remis. Cette réinitialisation doit, si le système le permet, être paramétrée de façon à forcer un changement du mot de passe par l'utilisateur, à la prochaine utilisation du système.	*	*	*
# 4.3 Outils utilisés				
10	Le personnel-DSN doit s'assurer de façon régulière que son poste de travail dispose bien de protections actives et à jour contre les programmes malveillants. Le personnel-DSN doit veiller à utiliser uniquement des outils réputés fiables sur le plan de la sécurité. Il évitera ainsi d'installer sur son poste et/ou sur un poste ayant des accès privilégiés, des outils risquant de comporter des logiciels espions, chevaux de Troie et autres programmes malveillants.	*		
11	Le personnel-DSN ne doit stocker aucun fichier sur son poste de travail susceptible de porter atteinte à la confidentialité du SI (que ce soit des données du SI, des fichiers d'utilisateurs, ou des informations sur les systèmes), ou dont l'altération/la destruction pourrait être pénalisante pour le SI. La panne ou le vol du poste de travail d'un personnel-DSN ne doit avoir aucune conséquence en matière de confidentialité ou de disponibilité.	*		
12	Le personnel-DSN ne doit pas laisser un poste, et notamment un poste de supervision, avec une connexion directe sur Internet (c'est-à-dire une connexion qui by-pass les éléments de sécurité : Pare feux, …).	*		
13	Le personnel-DSN ne doit jamais laisser hors de sa surveillance un poste sur lequel il s'est connecté. S'il quitte son poste, même temporairement, il doit a minima verrouiller ou fermer la session active.	*	*	*
14	Le personnel-DSN ne doit jamais faire sortir des locaux du CHU d'AMIENS PICARDIE des données du Système d'Information et/ou des fichiers comportant des informations relatives au S.I. Il faut utiliser les solutions de chiffrement : Bitlocker, 7-Zip, Zed ou de partage officiel : Cloudfile.	*	*	*
15	Le personnel-DSN doit tester toute évolution ou correction logicielle sur un environnement de test avant une mise en production. Il doit assurer une traçabilité de toutes les mises en production et décrire l'objet de l'évolution ou de la correction.		*	*
16	Le personnel-DSN doit documenter de façon claire, exhaustive et accessible aux personnels autorisés, tous les systèmes mis en place afin de permettre leur maintenance. Il documentera notamment avec soin les différentes architectures de sécurité mises en place : synoptiques, plans de nommage et d'adressage, politiques de filtrage, politique de disponibilité, politiques de sécurité des postes de travail etc. Toutes les documentations doivent être maintenues à jour.		*	*
# 4.4 Confidentialité et Réserve				
17	Le personnel-DSN a un devoir de réserve et de discrétion. Il est soumis au Secret Professionnel.	*		
18	Le personnel-DSN ne doit donner aucune information à des personnes	*	*	*

N°		Users	Adm CHU	Adm GHT HDS
	extérieures au service et/ou non habilitées, qui soit susceptible de porter atteinte à la sécurité du SI. Que ces informations portent sur l'architecture en place, sur des données du SI ou sur des projets de sécurisation.			
19	Le personnel-DSN assure le bon fonctionnement des conteneurs, hébergeurs et transporteurs de contenu. Il ne doit en aucune façon regarder ces contenus. S'il est amené de façon accidentelle, ou s'il est contraint, dans le cadre de sa mission et de façon exceptionnelle, à visualiser des informations confidentielles (nom ou contenu de fichiers, contenu de base de données, images…), il doit avoir une discrétion totale, écrite et orale, vis-à-vis de ces informations.	*	*	*
20	Le personnel-DSN n'a pas le droit de consulter des données personnelles des utilisateurs (espaces de fichiers mentionnés « privés » et messagerie dont l'objet est manifestement ou explicitement « personnel»). Il ne peut pas non plus communiquer ces données à la hiérarchie de l'utilisateur, sauf accord explicite de celui-ci, notamment lorsqu'un utilisateur quitte ou a quitté le CHU d'AMIENS PICARDIE. Les données non clairement identifiées comme « personnelles » des répertoires réseau individuels et partagés peuvent être communiquées à la hiérarchie du salarié, après accord du RSSI.	*		
21	Le personnel-DSN a le devoir de configurer et d'administrer les systèmes qu'il gère dans le sens d'une meilleure sécurité, dans l'intérêt des utilisateurs, et en accord avec le RSSI.	*	*	*
4.5 Surveillance				
22	Le personnel-DSN a le droit d'accéder, sur les systèmes qu'il administre, à des informations nécessaires à ses missions de diagnostic et d'administration (analyse de logs), en respectant scrupuleusement la confidentialité de ces informations.		*	*
23	La charte « Sécurité du Système d'Information » présente aux utilisateurs l'étendue des accès dont dispose la DSN, de par sa fonction. Sur demande d'un utilisateur, le personnel-DSN devra confirmer, en toute transparence, ces possibilités d'accès.	*	*	*
24	Le personnel-DSN a le droit d'établir des procédures de surveillance de toutes les tâches exécutées sur la machine, afin de déceler les atteintes ou les tentatives d'atteinte à la sécurité, après autorisation de sa direction et en accord avec le RSSI. La constitution de journaux doit être faite dans le respect des principes de la loi Informatique et Libertés.		*	*
25	Le personnel-DSN est responsable de la qualité de service des ressources qu'il a en charge et doit faire respecter les droits d'accès aux ressources. Pour assurer cette responsabilité et permettre le fonctionnement optimal de ces ressources, il peut être amené à prendre des dispositions telles que : arrêt de travaux, suppression de droits d'accès, verrouillage de fichiers, modification des espaces fichiers alloués, interdiction de flux à risque …	*		
4.6 Relation avec les tiers				
26	La venue d'un prestataire ponctuel dans le service doit être annoncée à l'ensemble du service par le personnel-DSN qui prend en charge ce prestataire, ils doivent tous porter un badge.	*		
27	Le personnel-DSN ne doit jamais laisser un prestataire extérieur ou un utilisateur extérieur à la DSN seul dans les locaux de la DSN.	*		
28	Le personnel-DSN doit, dans la mesure du possible, assurer une surveillance des prestataires connectés en télémaintenance sur un serveur ou un poste de télémaintenance, et il doit privilégier des ouvertures d'accès en télémaintenance à la demande. Il doit mettre en place une traçabilité de ces accès et réaliser, a posteriori, un reporting sur ces accès, afin d'être en mesure d'identifier des anomalies éventuelles.	*	*	*
29	Le personnel-DSN doit remettre des comptes individuels aux prestataires intervenant sur site. Ces comptes doivent être supprimés ou désactivés au	*	*	*

N°		Users	Adm CHU	Adm GHT HDS
	départ du prestataire. Ces comptes doivent disposer des droits minimum strictement nécessaires à l'exécution de leur mission. L'accès à des bases de données devra s'appuyer sur des comptes temporaires ou dont le mot de passe est changé au départ du prestataire.			
30	Le personnel-DSN ne doit pas remettre ni permettre à des sociétés prestataires/éditeurs des extractions de données réelles comportant des informations sensibles (qu'elles soient ou non nominatives), sauf contrat spécifique de confidentialité signé entre les parties.	*	*	*
4.7 Alerte				
31	Le personnel-DSN a le devoir de signaler au RSSI / RSMSI tout risque et tout incident susceptible de porter atteinte à la sécurité du Système d'Information et de l'infrastructure qui le supporte. Que cela provienne d'une panne, ou d'une malveillance ou une erreur de manipulation suspectée ou avérée.	*	*	*
4.8 Sécurité dans les projets				
32	Le personnel-DSN doit intégrer une étude sécurité dans tous les projets applicatifs et d'infrastructure. Pour chaque projet, une analyse de risque et des exigences sécurité doivent être établies par un groupe composé a minima du chef de projet DSN, du chef de projet utilisateur (si projet applicatif) et du RSSI / RSMSI. Si le projet donne lieu à une consultation auprès de sociétés extérieures, un volet sécurité reprenant ces exigences doit être intégré au Cahier des charges, puis, par la suite, au contrat adressé à ces sociétés. Pour les projets applicatifs, une « fiche sécurité application » doit être établie et doit être tenue à jour, depuis la phase d'étude jusqu'à la mise en production. Cette fiche est validée par le RSSI / RSMSI et elle est soumis en commission des projets validée par le RSN / DSN.	*		
33	Toute évolution dans la sécurité d'une application ou d'un élément de l'infrastructure doit être discutée avec le RSSI / RSMSI , validée par lui, puis documentée.	*	*	*