Sommaire

Version	Date d'actualisation	Modifications apportées (page / contenu)
1.0	15/09/2016	Création du document
2.0	13/06/2019	Mise à jour GHT – HOP'EN
3.0	10/11/2020	Mise à jour RGPD Modification de la nomination DSIT en DSN
4.1	12/09/2022	Validation

5.0	17/07/2023	Revue annuelle
5.1	25/10/2023	Validation de la Direction Générale

	Rédaction	Validation
Nom	Mickaël TAINE	COSSI
Date	15/09/2016	12/09/2022

1 Préambule

Dans un contexte d'accroissement des menaces et des cyberattaques à l'encontre du système de Soin français, le Centre Hospitalier Universitaire de Reims renforce sa démarche concernant la sécurité de l'information grâce à la construction d'un Système de Management de la Sécurité de l'Information (SMSI). Ainsi la donnée, son utilisation et sa protection doivent être au centre de la préoccupation de la sécurité numérique.

L'offre de soins de notre établissement s'appuie de plus en plus fortement sur un Système d'Information (SI) qui est devenu un outil indispensable à tous les professionnels pour :

- Le maintien de relations de confiance avec nos patients et nos partenaires ;
- L'amélioration continue de la prise en charge et de la qualité des soins prodigués aux patients ;
- La mise en œuvre de services toujours plus performants et adaptés aux besoins et pratiques de chacun ;
- La facilitation des coopérations avec l'ensemble des professionnels de santé partenaires.

Assurer la sécurité des Systèmes d'Information (SI) de l'établissement est dans ce contexte un enjeu fondamental pour :

- Respecter le contexte législatif et réglementaire ;
- Assurer aux patients la sureté des soins, la confidentialité et la pertinence de leurs informations ;
- Assurer aux professionnels de santé la disponibilité de leurs outils ;
- Préserver l'image de l'établissement et garantir la confiance des patients, des professionnels de santé et des institutions ;

C'est pourquoi la Direction Générale de l'établissement a décidé de mener une démarche axée sur la sécurité des Systèmes d'Information prenant en compte les contraintes et les exigences de ses activités, de ses professionnels et des patients.

Ce document de politique générale est le cadre de référence de cette démarche, où chacun contribuera activement à sa mise en œuvre en étant constamment un acteur de la sécurité des SI.

2 Orientations stratégiques

2.1 Des enjeux métiers majeurs

Établissement public de santé, le Centre Hospitalier Universitaire de Reims assure des missions de soin, d'enseignement et de recherche.

Afin de mener l'ensemble de ces missions en garantissant leur niveau d'excellence, le Centre Hospitalier Universitaire de Reims doit sans cesse répondre à des défis majeurs et notamment :

- Assurer la continuité des soins et les activités sensibles de l'établissement ;
- Améliorer la prise en charge du patient et la qualité des soins, ce qui rend nécessaire l'emploi de matériel médicotechnique perfectionné et interconnecté ou encore la présence d'une expertise médicale spécialisée et des possibilités de prise en charge pluridisciplinaire ;
- Respecter les droits du patient en garantissant la confidentialité, la traçabilité et la pérennité des données de santé au cours de leur cycle de vie dans le SI ;
- Assurer en toute circonstance l'identification fiable des patients pour garantir la qualité de leur prise en charge et la sécurité des soins qui leurs sont prodigués ;
- Proposer un environnement optimisé et ouvert pour les travaux de recherche, d'enseignement et de collaboration avec d'autres structures ;
- Maintenir l'équilibre budgétaire et rechercher en permanence des optimisations des processus périphériques à la production de soins ;
- Assurer ses rôles d'établissement support du Groupement Hospitalier de Territoire.

2.2 Le Système d'Information : un élément essentiel des processus métiers

Avec la modernisation des systèmes d'information hospitaliers notamment en matière de e-santé, les processus métiers reposent de manière structurante sur des briques du Système d'Information de Santé, en particulier pour :

- La mise en œuvre du Dossier Patient Partagé en interne voire au sein d'une communauté médicale plus large que celle composant le Centre Hospitalier Universitaire de Reims ;
- La mise en œuvre du Dossier Médical Personnel (ou DMP, lancé par la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie) ;
- La mise en œuvre de Mon Espace Santé (décret n°2021-10483 relatif à la mise en œuvre de l'espace numérique de santé qui prévoit la création automatique des comptes Mon espace santé) ;
- La dématérialisation des processus métiers : gestion des prescriptions, gestion des soins, imagerie médicale et compte-rendu des examens (PACS), etc. ;
- L'ouverture et le partage d'information avec d'autres établissements ou professionnels de santé : e-santé, téléconsultation, télé-imagerie, interventions à distance, etc.

Le Système d'Information constitue une ressource stratégique et vitale pour le bon fonctionnement du Centre Hospitalier Universitaire de Reims. Sa fiabilité est donc essentielle pour répondre aux besoins des patients, de l'ensemble des professionnels de santé et de l'administration.

2.3 Le contexte juridique et règlementaire

Le Centre Hospitalier Universitaire de Reims évolue dans un environnement juridique et règlementaire riche relatif à son Système d'Information, qu'il se doit de respecter. Le cadre législatif récent est particulièrement exigeant sur la Sécurité du Système d'Information, et en particulier pour les informations de santé à caractère personnel :

- Décret de confidentialité relatif à la confidentialité des données médicales : Décret n°2007-960 du 15 Mai 2007 ;
- Référentiel Général de Sécurité (RGS) nécessitant une homologation formelle des téléservices : Décret n°2010-112 du 2 février 2010 ;
- Arrêté du 25 mars 2010 portant désignation des Autorités Qualifiées pour la Sécurité des Systèmes d'Information (AQSSI) dans les établissements de santé ;
- Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) de Juillet 2013 ;
- Directive NIS (Network and Information System Security) (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 ;
- Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique ;
- Arrêté du 14 septembre 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique ;
- Règlement Général sur la Protection des Données (RGPD - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016) ;
- Loi informatique et Libertés : Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifiée) ;

La Politique Générale de Sécurité du Système d'Information du Centre Hospitalier Universitaire de Reims se doit donc de proposer un cadre en cohérence avec l'ensemble de ces exigences.

2.4 La Sécurité du Système d'Information : une priorité au service des enjeux métiers

Le Système d'Information est une ressource particulièrement vulnérable, exposée à de nombreux risques, qui peuvent résulter d'actes de malveillance (fraude, divulgation d'information, attaque par déni de service…), d'erreurs (en phase de conception, d'exploitation ou en cours d'utilisation), d'accidents (incendie, dégâts des eaux, panne technique…) ou encore de manque de maîtrise (départ de personnes clés par exemple). Ces risques peuvent conduire à des dysfonctionnements graves au sein du Centre Hospitalier Universitaire de Reims, ayant potentiellement des impacts importants sur la prise en charge du patient et la qualité des soins, des impacts en termes d'image et susceptible de perte de confiance dans les espaces numériques de santé.

La Sécurité du Système d'Information a pour finalité de garantir la maîtrise de ces risques dans le but de créer un espace numérique de confiance apte à accueillir et à traiter des données de santé. Elle conditionne l'adhésion des professionnels de santé et la confiance des patients.
Elle s'impose donc comme une composante essentielle de la protection du Système d'Information du Centre Hospitalier Universitaire de Reims, et assure :

- La **Disponibilité** du Système d'Information et des données de santé, et en particulier dans le cas d'applications supportant des processus métiers vitaux (exemple : Urgences) ;
- L'**Intégrité** des informations et des moyens de la traiter, qui est primordiale pour attester de l'exactitude et de la fiabilité des opérations ;

- La **Confidentialité** des informations, et en particulier des données à caractère personnel et des données protégées par le secret médical ;
- La **Traçabilité**, afin d'assurer l'imputabilité des actions (exemple : prescriptions médicales).

2.5 Rôle de la Politique Générale de Sécurité du Système d'Information

La Politique Générale de Sécurité du Système d'Information constitue le **cadre de référence** pour la mise en œuvre de la Sécurité du Système d'Information au sein du Centre Hospitalier Universitaire de Reims. Elle se fonde sur une analyse de risques, qui doit faire l'objet de mises à jour régulières. Ainsi, elle formalise l'ensemble des éléments stratégiques, de l'organisation, de la démarche, des principes et des règles de sécurité ayant comme objectif la protection du Système d'Information.
Elle assure :

- L'intégration de la Sécurité du Système d'Information dans la vision stratégique de la gestion globale des risques du Centre Hospitalier Universitaire de Reims ;
- La mise en évidence des objectifs, obligations et engagements du Centre Hospitalier Universitaire de Reims vis-à-vis de ses patients et de ses partenaires ;
- La promotion de la coopération entre les différents services du Centre Hospitalier Universitaire de Reims pour l'élaboration et la mise en œuvre des mesures, consignes et procédures ;
- L'assurance de la cohérence et de la pérennité des actions de sécurité ;
- La sensibilisation aux risques menaçant le SI et aux moyens disponibles pour s'en prémunir ;
- Une gradation des moyens, avec une proportionnalité assurée par l'analyse de risque ;
- Une aide aux Directions Métiers, notamment la Direction des Services Numériques, et aux chefs de projets pour intégrer la Sécurité du Système d'Information au plus tôt dans les développements de nouveaux services ;
- Une explicitation des principes de sécurité à appliquer dans l'ensemble des établissements constituant le Groupement Hospitalier de Territoire pour lequel le Centre Hospitalier Universitaire de Reims est l'établissement support, afin d'assurer une application homogène de ces règles en son sein.

3 La Politique Générale de Sécurité du Système d'Information

3.1 Périmètre d'applicabilité

La Politique Générale de Sécurité du Système d'Information couvre l'ensemble des informations et leur traitement (création, conservation, échange, etc.), quelle que soit la forme matérielle ou immatérielle sous laquelle elles sont exploitées (électronique, imprimée, manuscrite, vocale, image …).

Elle concerne l'ensemble des activités du Centre Hospitalier Universitaire de Reims, de ses partenaires et des sous-traitants, quels que soient leurs lieux d'implantation. Elle s'applique également à l'ensemble des établissements composant le Groupement Hospitalier de Territoire pour lequel le Centre Hospitalier Universitaire de Reims est l'établissement support.

Elle porte sur l'ensemble des ressources du Système d'Information, c'est-à-dire :

- L'ensemble des processus et modes opératoires de protection des informations et des traitements ;
- L'ensemble du cycle de vie du Système d'Information et de ses composants ;
- L'ensemble des composants matériels et logiciels du Système d'Information, en particulier :
  - Les applications, processus de traitement, bases de données et les serveurs qui les hébergent ;
  - Les réseaux de communication (particulièrement les interconnexions avec les partenaires et prestataires) ;
  - Les moyens et environnements techniques de fonctionnement des équipements ;
- L'ensemble des processus et modes opératoires de production et d'échange d'informations, quelle qu'en soit la nature (données, voix, images) ;
- Les bâtiments et locaux hébergeant les ressources informatiques.

Elle s'applique à toute personne physique ayant accès au Système d'Information du Centre Hospitalier Universitaire de Reims, ou toute personne morale qu'elle soit une entité administrative ou privée, qu'elle soit interne ou externe à l'établissement (sous-traitant, stagiaire, prestataire). Elle s'impose à tous et nécessite l'engagement de chacun.
Elle doit être transposée dans les contrats ou les marchés au titre desquels le Centre Hospitalier Universitaire de Reims donnerait accès à son Système d'Information. Les services sont chargés, à cette fin, de les décliner dans les documents contractuels qu'ils sont amenés à élaborer.

3.2 Structure de la Politique Générale de Sécurité du Système d'Information

La Politique Générale de Sécurité du Système d'Information du Centre Hospitalier Universitaire de Reims est formalisée dans un référentiel documentaire à plusieurs niveaux :

- Le présent document, la **Politique Générale**, en constitue le premier niveau.

  Il décrit le cadre de référence en matière de Sécurité du Système d'Information en fixant les enjeux et les principes de gouvernance. Il détermine également les principes fondamentaux et les grandes orientations en matière de sécurité, en conformité avec la Politique Ministérielle de Sécurité des Systèmes d'Information, les principes fondateurs de la Politique Générale de Sécurité des Systèmes d'Information de Santé et les différentes thématiques des normes ISO 27 001 et ISO 27 002 ;
- Un corpus documentaire de **politiques thématiques** déclinées selon les normes ISO 27 001 et ISO 27 002.

  Il définit dans le détail les processus et règles de sécurité à mettre en œuvre par thématique de sécurité.
- L'ensemble des politiques opérationnelles sont décrites dans le document : « RS_Politique_PGSSI_PO_V1.3 ».
- Des chartes d'utilisation du Système d'Information, dont notamment la Charte informatique ;
- Des procédures opérationnelles ou techniques ;

  Ces procédures opérationnelles et techniques viennent compléter la politique opérationnelle, dans des environnements techniques spécifiques.

3.3 Mise en application

La Politique Générale de Sécurité du Système d'Information (PGSSI), validée et signée par l'Autorité Qualifiée pour la Sécurité du Système d'Information (AQSSI) du Centre Hospitalier Universitaire de Reims, est diffusée à l'ensemble du personnel de l'établissement en charge de son application.
Les règles de sécurité de la PGSSI sont également diffusées aux tierces parties en relation avec l'organisation du Centre Hospitalier Universitaire de Reims lorsqu'elles sont concernées.
L'application de ces règles fait l'objet d'une mise en œuvre progressive et par paliers, suivant une logique d'amélioration continue. Les actions permettant d'atteindre chacun de ces paliers sont déterminées et sélectionnées en conformité avec la cible définie par l'analyse de risque conduite par l'établissement.

3.4 Mise à jour de la Politique Générale de Sécurité du Système d'Information

La Politique Générale de Sécurité du Système d'Information du Centre Hospitalier Universitaire de Reims fera l'objet d'une révision annuelle.

4 Organisation de la sécurité du Système d'Information

L'organisation fonctionnelle de la Sécurité du Système d'Information, conformément aux recommandations ministérielles, permet de prendre en compte les exigences de sécurité au plus haut niveau de l'établissement. Elle est principalement composée de :

- L'AQSSI, ou Autorité Qualifiée pour la Sécurité du Système d'Information, assure la responsabilité globale de la Sécurité du Système d'Information pour le Centre Hospitalier Universitaire de Reims. L'AQSSI apprécie l'ensemble des risques de Sécurité du Système d'Information inhérents aux activités du Centre Hospitalier Universitaire de Reims et alloue les budgets nécessaires à leur traitement. Elle délègue ses missions à l'Autorité d'Appui (AA) ;
- Le RSSI, ou Responsable de la Sécurité du Système d'Information, assiste l'AQSSI et est l'animateur de la démarche de sécurité. Le RSSI s'assure de la mise en application des exigences métiers sur le périmètre du Système d'Information et de la démarche de management de la Sécurité du Système d'Information avec l'appui de l'équipe sécurité de la Cellule Qualité & Sécurité.
- Les Pôles, Directions ou Délégations métiers, intégrant l'ensemble de la population médicale, paramédicale, technique ou administrative, définissent leurs exigences et leurs besoins en termes de Sécurité du Système d'Information.
- La Direction des Services Numériques, est la maîtrise d'œuvre de la Sécurité du Système d'Information. Elle assure le maintien en condition opérationnelle de la Sécurité du Système d'Information et pilote le niveau de service des prestataires informatiques.

4.1 Autorité Qualifiée pour la Sécurité du Système d'Information (AQSSI)

Le **Directeur Général du Centre Hospitalier Universitaire de Reims** est nommé par arrêté ministériel Autorité Qualifiée pour la Sécurité du Système d'Information (AQSSI)), et en délègue les missions au Directeur des Services Numériques, qui est à cet égard Autorité d'Appui (AA).

L'AQSSI assure la responsabilité globale de la Sécurité du Système d'Information pour le Centre Hospitalier Universitaire de Reims. Elle porte l'ensemble des risques liés à la Sécurité du Système d'Information, et est

responsable de la bonne application des mesures de Sécurité du Système d'Information. A ce titre, elle doit notamment :

- S'assurer de la bonne application des dispositions ministérielles définies dans la Politique Ministérielle de Sécurité du Système d'Information et plus largement du contexte législatif et réglementaire applicable ;
- Disposer d'une analyse des risques sur le Système de Management de la Sécurité de l'Information ;
- Définir la Politique Générale de Sécurité du Système d'Information, en cohérence avec la Politique Ministérielle de Sécurité des Système d'Information et la Politique Générale de Sécurité des Systèmes d'Information de Santé ;
- S'assurer que les dispositions réglementaires et contractuelles sur la Sécurité du Système d'Information, en particulier avec des tiers, soient appliquées ;
- Elaborer les directives internes et désigner ou valider les acteurs de la filière sécurité chargés des diverses tâches liées à la Sécurité du Système d'Information ;
- S'assurer que les contrôles internes de sécurité soient régulièrement effectués ;
- Sensibiliser et former le personnel aux questions de sécurité ;
- Veiller à l'application des règles de sécurité, y compris par les entreprises contractantes, pour la protection et le contrôle des personnels, notamment dans les domaines liés aux droits d'accès, à l'habilitation et au respect de la vie privée ;
- S'assurer que tout système d'information, avant sa mise en service, ait fait l'objet d'une homologation ;
- Apporter sa contribution aux plans de lutte interministériels contre le cyberterrorisme, en prenant notamment en compte les avis ou alertes émis par le centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR et CERT-SANTE) ;
- Rendre compte immédiatement aux autorités et au CERT-FR et CERT-SANTE de tout incident et de tout phénomène suspect pouvant affecter la Sécurité du Système d'Information avec, si besoin, un régime d'astreinte approprié ;
- Remonter sans délai, conformément à la loi de santé, les incidents graves de sécurité des systèmes d'information à l'agence régionale de santé.

L'AQSSI est représentée par une Autorité d'Appui (AA) et délègue la mise en œuvre opérationnelle de la démarche au Responsable de la Sécurité du Système d'Information (RSSI). La désignation d'une AA ou d'un RSSI est accompagné d'une lettre de mission signée par l'AQSSI, et transmise aux autorités, conformément aux exigences de la Politique Ministérielle de Sécurité des Système d'Information.

4.2 Autorité d'Appui (AA)

Le Directeur des Services Numériques est désigné, par lettre de mission, Autorité d'Appui (AA) par l'AQSSI. L'Autorité d'Appui représente l'AQSSI dans l'exercice de ses responsabilités en matière de Sécurité du Système d'Information. L'Autorité d'Appui dispose de la vision stratégique du Centre Hospitalier Universitaire de Reims et peut représenter l'AQSSI au sein des différentes instances traitant de Sécurité du Système d'Information.

4.3 Responsable de la Sécurité du SI (RSSI)

Le Responsable de la Sécurité du Système d'Information est nommé par lettre de mission par l'AQSSI. Il est responsable de la mise en application de la Politique Générale de Sécurité du Système d'Information, ainsi que des

processus et des dispositifs en découlant. Il s'assure de la conformité du Système d'Information aux obligations légales, réglementaires et à la Politique Générale de Sécurité du Système d'Information.

Le RSSI a pour principales missions de :

- S'assurer que la Politique de Sécurité des Systèmes d'Information de l'établissement est définie et validée par la Direction Générale, et mise à jour a minima tous les ans au sein de la structure. Le RSSI est, par ailleurs, responsable de la mise en place de l'organisation en charge de l'animation de la SSI et de la mise en œuvre de la PGSSI sur le Système d'Information de l'établissement ;
- Veiller à ce qu'une analyse des risques de la sécurité des systèmes d'information soit menée au sein de l'établissement ;
- Mettre en œuvre la Politique de sécurité des systèmes d'information définie au sein de l'établissement ;
- S'assurer de la mise en œuvre de manière homogène de la Politique de sécurité des systèmes d'information au sein du Groupement Hospitalier de Territoire, en lien avec le porteur de la fonction Sécurité des Systèmes d'Information de chaque établissement ;
- Choisir des mesures de sécurité, élaborer le plan de mise en œuvre et suivre la mise en place des mesures de sécurité ;
- Auditer et contrôler l'application des règles de la Politique de sécurité des systèmes d'information au sein de l'établissement et, le cas échéant, d'alerter l'AQSSI en cas de défaut d'application de cette Politique ;
- Assurer la communication sur la démarche sécurité auprès de la Direction, des instances et des utilisateurs de l'établissement, sur leurs responsabilités et leurs usages du système d'information ;
- Surveiller et gérer les incidents de sécurité au sein de l'établissement ;
- Assurer la veille technique, réglementaire et institutionnelle en matière de sécurité des systèmes d'information de santé et plus largement en matière de SSI.

4.4 Pôles, Directions ou Délégations Métiers

Les **Pôles, Directions ou Délégations Métiers** du Centre Hospitalier Universitaire de Reims, intégrant l'ensemble de la population médicale, paramédicale, technique et administrative sont les maîtrises d'ouvrage de la Sécurité du Système d'Information.

Ils ont pour mission de :

- Définir les responsables des données qu'elles gèrent ;
- Exprimer leurs exigences et leurs besoins de sécurité et en particulier pour la continuité des activités, en accord avec leurs enjeux et les moyens accordés aux projets ;
- Mettre en œuvre des modes dégradés métiers pour les activités critiques afin de pallier tout sinistre informatique majeur.

4.5 Direction des Services Numériques

La Direction des Services Numériques est le pôle d'activité métier ayant la charge de la maîtrise d'œuvre de la Sécurité du Système d'Information. Elle a pour mission de :

- Assurer la bonne prise en compte des besoins de sécurité métiers et la mise en œuvre des mesures de sécurité qui en découlent ;
- Instruire les problématiques de sécurité dans l'ensemble des chantiers selon les processus et procédures mises en place par le RSSI ;
- Participer à la définition et à la mise en œuvre du Plan de Reprise d'Activité du Système d'Information ;
- Contribuer à l'élaboration des procédures opérationnelles et techniques sécurité ;
- Suivre et assurer la mise en œuvre des plans d'action sécurité ;
- Opérer la sécurité au quotidien, et assurer le maintien en condition opérationnelle du Système d'Information conformément à la Politique Générale de Sécurité du Système d'Information et aux bonnes pratiques ;
- Effectuer les contrôles de sécurité opérationnelle ;
- Informer le RSSI de toute problématique de sécurité rencontrée et de tout incident avéré ou suspecté.

La Direction des Services Numériques peut faire appel à des tiers pour réaliser certaines tâches qu'elle ne pourrait assurer par elle-même. Dans ce cas, elle doit :

- Valider la prise en compte des besoins de sécurité des métiers lors de la mise en œuvre des projets par le sous-traitant ;
- S'assurer de l'existence et du respect des engagements de service des sous-traitants ;
- Mettre en œuvre les interfaces nécessaires entre les processus de sécurité du sous-traitant et ceux du Centre Hospitalier Universitaire de Reims.

4.6 Autres Acteurs

4.6.1 Utilisateur

Chaque utilisateur a la responsabilité d'appliquer les règles de Sécurité du Système d'Information, mais également d'adopter un comportement limitant les risques. A ce titre, les utilisateurs s'engagent en particulier à respecter la charte informatique du système d'information. Ils se doivent, par déontologie, d'informer l'AQSSI, l'AA ou le RSSI de tout incident, anomalie et infraction à la Politique Générale de Sécurité du Système d'Information ou aux règles d'application portées à sa connaissance.

4.6.2 Direction juridique

La Direction des Affaires Juridiques a une mission de veille et de conseil, des aspects législatifs, réglementaires et déontologiques ayant trait à la Sécurité du Système d'Information. Elle fournit les informations permettant à chaque collaborateur d'exercer son activité conformément à la réglementation en vigueur.

4.6.3 Délégué à la Protection des Données (DPD)

Conformément au Règlement Général sur la Protection des Données (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016) et à la loi relative à l'informatique, aux fichiers et aux libertés, un Délégué à la Protection des Données (DPD) est désigné au sein du Centre Hospitalier Universitaire de Reims. Il contribue à la définition des besoins de sécurité des systèmes d'information des lors que ceux-ci traitent des données à caractères personnel.

Le DPD a pour principales missions :

- D'informer et de conseiller l'AQSSI, ainsi que l'ensemble du personnel de l'établissement, sur les obligations définies par le Règlement Général de Protection des Données (RGPD) et par les autres dispositions en matière de protection de données à caractère personnel ;
- D'informer, si besoin, des manquements constatés, de conseiller dans les mesures à prendre pour y remédier, de soumettre les arbitrages nécessaires
- De veiller à la mise en œuvre de mesures appropriées pour permettre de démontrer que les traitements sont effectués conformément au RGPD, et si besoin, réexaminer et actualiser ces mesures ;
- De veiller à la bonne application du principe de protection des données dès la conception et par défaut dans tous les projets comportant un traitement de données personnelles
- D'auditer et contrôler, de manière indépendante, le respect du RGPD par l'établissement, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement et les audits s'y rapportant;
- De piloter la production et la mise en œuvre de politiques, de lignes directrices, de procédures et de règles de contrôle pour une protection efficace des données personnelles et de la vie privée des personnes concernées ;
- D'assurer la bonne gestion des demandes d'exercice de droits, des réclamations et des requêtes formulées par les personnes concernées par nos traitements, d'assurer leur transmission aux services intéressés et apporter à ces derniers un conseil dans la réponse à fournir aux requérants;
- Être l'interlocuteur privilégié de l'autorité de contrôle et coopérer avec elle ;
- Dispenser des conseils en ce qui concerne les études d'impact sur la vie privée et en assurer la pertinence
- De mettre l'établissement en position de notifier d'éventuelles violations de données auprès de l'Autorité de contrôle et de porter conseil à l'AQSSI, notamment concernant les éventuelles communications aux personnes concernées et les mesures à apporter ;
- De tenir l'inventaire et documenter les traitements de données à caractère personnel en tenant compte du risque associé à chacun d'entre eux compte-tenu de sa nature, sa portée, du contexte et de sa finalité.

4.6.4 Administrateurs du Système d'Information

Les administrateurs du Système d'Information possèdent des droits qui leur permettent d'accéder à tout ou partie du Système d'Information. Ce type de privilèges ne peut être utilisé que dans le cadre d'une action réelle d'administration encadrée par la charte Administrateur. Les administrateurs du Système d'Information doivent également exercer une surveillance permanente et informer l'AQSSI et le RSSI selon la charte Administrateur définie.
En dehors d'une action d'administration, les administrateurs se trouvent être des utilisateurs du Système d'Information avec les mêmes droits et devoirs.

4.6.5 Direction des Ressources Humaines

La Direction des Ressources Humaines veille à l'intégration de la Sécurité du Système d'Information tout au long de la collaboration avec les agents : avant le contrat, pendant l'exécution du contrat et lors de la fin de contrat.

4.7 Animation et coordination de la Sécurité du Système d'Information

4.7.1 Comité Stratégique de Sécurité du Système d'Information

Le Comité Stratégique de Sécurité du Système d'Information aura lieu annuellement et a pour objectif de :

- Valider la Politique Générale de Sécurité du Système d'Information et ses évolutions ;

Le Comité Stratégique de Sécurité du Système d'Information est présidé par l'AQSSI ou son AA et est animé par le RSSI.

4.7.2 Commission de la Stratégie Numérique

La commission de la stratégie numérique est biannuelle et a pour objectif de :

- Valider les plans d'action et les budgets en matière de Sécurité du Système d'Information ;
- Piloter les actions de sécurité au travers de tableaux de bord.

4.7.3 Comité Opérationnel de Sécurité du Système d'Information

Le Comité Opérationnel de Sécurité du Système d'Information est mensuel. Il a pour objectif de :

- Suivre régulièrement des mesures de sécurité ;
- Suivre les incidents de sécurité et la définition des mesures d'amélioration ;
- Suivre les projets de sécurité du système d'information ;
- S'assurer de la prise en compte de la PGSSI dans tous les projets SI

Le Comité Opérationnel de Sécurité du Système d'Information est dirigé par le RSSI et est composé essentiellement de responsable d'équipes de la Direction des Services Numériques.

5 Principes de sécurité

Les principes de sécurité listés ci-dessous sont basés notamment sur les principes fondateurs de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) et sur les bonnes pratiques informatiques diffusées par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

5.1 Principes structurants de la politique

Les responsabilités et règles présentées dans le corpus documentaire sécurité reposent sur les principes suivants :

- Tout accès à des informations qui ne seraient pas publiques nécessite une habilitation ;
- Tout accès aux Systèmes d'Information Essentiels, qui n'est pas explicitement autorisé, est interdit (principe du moindre privilège) ;
- Les droits d'accès sont personnels, attachés à un rôle, incessibles et ne sont pas permanents ;
- Les utilisateurs n'accèdent qu'aux informations nécessaires (principe du besoin d'en connaître) ;
- Les informations manipulées ou gérées sont classifiées afin d'adapter les mesures de sécurité aux réels enjeux et risques ;
- Les données de santé à caractère personnel, notamment les informations permettant l'identification des patients doivent faire l'objet d'une attention particulière pour garantir leur disponibilité, leur intégrité et leur confidentialité ;
- La mise en place et le maintien de l'efficacité de tout moyen de sécurité impliquent un contrôle régulier à l'aide d'éléments tangibles ;
- La sécurité globale d'un système étant toujours celle du composant le plus faible, la sécurité s'applique de manière cohérente à l'ensemble du système d'information de l'établissement (principe de cohérence) ;
- Tous les moyens doivent être mis en œuvre afin d'identifier tous les incidents de sécurité, d'en mesurer les impacts, afin de les contrôler, les réparer et éviter leur reproduction.

5.2 Présentation du corpus documentaire selon le profil des utilisateurs

Thèmes ISO 27001 et Annexe A	Politiques	Agents CHU de Reims			Professionnels tiers	
		Utilisateur avec droits à privilège	Utilisateur sans droit à privilège	Pilote de processus	Accès avec droits à privilège	Accès sans droit à privilège
Contexte de l'organisation	Politique Générale de Sécurité du Système d'Information	X	X	X	X	X
Evaluation des performances	Audit des systèmes d'information	X		X	X	
Organisation de la sécurité de l'information	Charte du télétravail, Politique de Gestion du Télétravail, Charte d'Utilisation des Smartphones Professionnels. Politique Opérationnelle	X	X	X	X	X
Gestion des actifs	Gestion des actifs et transfert de données	X	X	X	X	X
Contrôle d'accès	Politique de contrôle d'accès	X	X	X		
Cryptographie	Développement & Cryptographie	X	X	X	X	X
Sécurité physique et environnementale	Contrôle et accès de la sécurité physique et environnementale	X	X	X	X	X

Sécurité liée à l'exploitation	Gestion des évènements	**X**		**X**	**X**	
Sécurité des communications	Gestion des actifs et transfert de données	**X**		**X**		
Acquisition, développement et maintenance des systèmes d'information	Développement & Cryptographie Politique Opérationnelle	**X**		**X**		
Relations avec les fournisseurs	Gestion des fournisseurs	**X**		**X**	**X**	**X**
Gestion des incidents liés à la sécurité de l'information	Gestion des incidents liés à la sécurité de l'information	**X**		**X**		
Aspects de la sécurité de l'information dans la gestion de la continuité d'activité	PCA/PRA	**X**		**X**		

6 Approche par les risques

Le système d'information, par les vulnérabilités des ressources qui le compose (matériels, logiciels, personnes, outils internes, données, documents), est exposé à des menaces pouvant causer des préjudices graves sur l'intégrité, la confidentialité, la disponibilité et la traçabilité des données de l'organisation.

Pour remédier à ces vulnérabilités de manière optimisée, il est nécessaire de suivre une approche basée sur les risques décrite ci-dessous :

- Identifier le patrimoine informationnel
- Identifier les actifs
- Identifier les vulnérabilités
- Identifier les menaces
- Identifier les scenarios de risques

- Évaluer et choisir le traitement des risques
- Définir le plan d'action
- Déterminer et accepter les risques résiduels

- Définir l'échelle d'impact
- Définir l'échelle de probabilité
- Définir l'échelle d'acceptation du risque

- Évaluer les besoins de sécurité
- Évaluer les probabilités
- Apprécier les risques

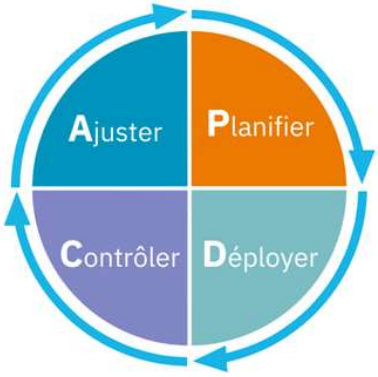
Cette approche de gestion par les risques permet notamment :

- D'identifier et d'évaluer les risques majeurs menaçant le système d'information ;
- D'expliciter les responsabilités des acteurs en charge du traitement des risques ;
- De définir avec les propriétaires des risques, les mesures de traitement des risques identifiés.
- De formaliser les principes de sécurité régissant la protection du système d'information ;
- D'établir les règles de sécurité minimales à respecter ;
- D'élaborer ou de mettre à jour la politique opérationnelle et les politiques de sécurité thématiques.

6.1 Amélioration continue

En plus de l'approche basée sur les risques, la mise en œuvre d'un système de management de la sécurité de l'information s'appuie sur le principe d'amélioration continue. Ce principe est basé sur le modèle PDCA issu de la norme ISO 27001.

Il repose sur la vérification de l'adéquation d'un déploiement avec un résultat attendu. En cas d'objectif non atteint, il implique la réalisation d'une analyse et d'un plan de correction afin de capitaliser sur les erreurs passées.



CERCLE VERTUEUX DU PDCA

Planifier : Etablir la politique, objectifs, processus et procédures relatifs à la gestion du risque et à l'amélioration de la sécurité de l'information de manière à fournir des résultats conformément aux politiques et aux objectifs globaux.
Déployer : Mettre en œuvre et exploiter la politique, les mesures, les processus et les procédures.
Contrôler : Evaluer les performances des processus par rapport à la politique, aux objectifs et à l'expérience pratique et rendre compte des résultats à la direction pour réexamen.
Ajuster : Entreprendre les actions correctives et préventives, sur la base des résultats de l'audit interne et de la revue de direction.

7 Annexes

7.1 Rappel des définitions

- Une **information** est constituée par tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.
- Un **système d'information (SI)** est un ensemble organisé d'éléments qui permet de regrouper, de classifier et de diffuser de l'information sur un phénomène donné. C'est donc l'ensemble des moyens humains et matériels ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire l'information, au sein d'une même organisation et dans ses relations avec l'extérieur.
- La **sécurité de l'information** est un processus visant à assurer la disponibilité des informations et à les protéger contre l'accès, l'utilisation, la diffusion, la destruction, ou la modification non autorisée. Elle s'applique à tous les aspects de la sûreté, de la garantie, et de la protection d'une information, quelle que soit sa forme. La sécurité de l'information n'est donc pas confinée aux seuls systèmes informatiques, ni à l'information dans sa forme numérique ou électronique.
- La **sécurité des systèmes d'information (SSI)** est assurée par l'ensemble des moyens juridiques, organisationnels, techniques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité de l'information.
- Le **Système de Management de la Sécurité de l'Information (SMSI)** est l'ensemble des politiques de sécurité, des moyens de pilotage et de contrôle, des processus et des outils permettant de gérer et de maîtriser les risques liés à la sécurité de l'information. Le SMSI fait partie d'une démarche d'amélioration continue et intègre les évolutions de l'établissement pour toujours maintenir un niveau d'efficacité optimal.

7.2 Glossaire

AA	Autorité d'Appui
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AQSSI	Autorité Qualifiée pour la Sécurité des Systèmes d'Information
CERT-FR	Centre Gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
CERT-SANTE	Centre Gouvernemental de veille, d'alerte et de réponse aux attaques informatiques aux établissements de santé, aux organismes et services médico-sociaux
DICT	Disponibilité, Intégrité, Confidentialité, Traçabilité
DPD	Délégué à la Protection des Données
DSN	Direction des Services Numériques
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
HDS	Hébergeur de Données de Santé
OSE	Opérateur de Services Essentiels
NIS	Network and Information Security
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PMSSI	Politique Ministérielle de Sécurité des Systèmes d'Information
PGSSI	Politique Générale de Sécurité du Système d'Information
RGI	Référentiel Général d'Interopérabilité
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité

RSSI	Responsable de la Sécurité du Systèmes d'Information
SI	Système d'Information
SMSI	Système de Mangement de la Sécurité de l'Information
SSI	Sécurité du Systèmes d'Information

7.3 Références

- Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) de Juillet 2013 ;
- Référentiel général de sécurité
- EBIOS RM 2018 - Expression des Besoins et Identification des Objectifs de Sécurité – ANSSI
- Guide d'intégration de la sécurité des systèmes d'information dans les projets – ANSSI
- Guide d'élaboration de politiques de sécurité des systèmes d'information – ANSSI
- ISO 27001 - Système de Management de la Sécurité de l'Information (SMSI)
- ISO 27002 - Code de bonnes pratiques pour la gestion de la sécurité de l'information
- ISO 27018 - Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public
- ISO 20 000-1 - Exigences du système de management des services
- Arrêté du 14 septembre 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

Signé électroniquement par
Laetitia MICAELLI FLENDER
Le 26/10/2023 à 12:30