Titre	Politique générale de Sécurité de l'Information		No : 2024-A-058-r0
Direction responsable	Direction des ressources informationnelles, stratégies numériques et génie biomédical		
Applicable à	Centre Hospitalier Universitaire Sainte-Justine et la Fondation		
Nom du signataire	Nathan Lavigueur		
Signature	Nathan Lavigueur (Mar 13, 2024 09:35 EDT)		
En vigueur le	2024-02-27	**Révisé le**	

1 Contexte

Le Centre hospitalier universitaire de Sainte-Justine (ci-après le CHUSJ) est un établissement de santé public engagé envers l'excellence des soins prodigués à ses patients. Conscient du caractère sensible des informations qu'il détient et manipule dans le cadre de sa mission, le CHUSJ doit conséquemment, dans le cadre légal qui lui est applicable, assurer la confidentialité, l'intégrité et la disponibilité de ces informations afin, notamment, de protéger ses patients, son personnel et ses partenaires.

L'indisponibilité, l'altération ou la divulgation non autorisée de l'information peut provoquer des conséquences graves, allant jusqu'à compromettre le fonctionnement de services essentiels, occasionner d'importantes pertes financières, éroder la réputation du CHUSJ, et potentiellement mettre en danger la vie privée, la santé ou la sécurité des individus.

Il est donc nécessaire d'élaborer un ensemble cohérent de mesures pour garantir une protection adéquate des actifs informationnels supportant ces informations sensibles. Ces mesures doivent tenir compte de la valeur de l'information ainsi que des obligations du CHUSJ. Il est essentiel de mettre en œuvre des mesures de protection appropriées tout au long du cycle de vie de l'information.

2 Portée

La présente politique s'applique à l'ensemble des utilisateurs de l'information au sein du CHUSJ, englobant les dirigeants, le personnel de tous statuts, et toute personne physique agissant en tant que patient, consultant, médecin, chercheur, partenaire, fournisseur ou visiteur ayant accès aux

actifs informationnels du CHUSJ. Elle inclut également toute personne dûment autorisée à accéder à ces informations, et s'applique notamment par extension à la Fondation Sainte-Justine.

Les informations visées par cette politique englobent celles détenues par le CHUSJ dans le cadre de sa mission, qu'elles soient conservées en interne ou par des tiers, et concernent des formats tant numériques que non numériques.

Les activités concernées par cette politique englobent toutes celles qui impliquent l'utilisation, la transmission ou la conservation, sous quelque forme que ce soit, d'un actif informationnel appartenant ou détenu par le CHUSJ, sans égard aux supports ou aux emplacements, qu'elle soit exercée dans les locaux de cette dernière, ou un autre lieu, tout au long du cycle de vie de l'actif.

3 Objectifs

Cette politique exprime la vision stratégique du CHUSJ sur la protection des actifs informationnels critiques pour sa mission, sa crédibilité et ses relations avec les patients, fournisseurs, partenaires et son personnel. Elle assure la conformité légale, notamment la protection des renseignements personnels (ci-après PRP) et la vie privée. Elle constitue la pierre angulaire définissant les orientations et principes, mais vise également l'amélioration continue de la sécurité de l'information tout en restant alignée sur les objectifs opérationnels du CHUSJ.

Ainsi, la présente politique doit permettre de :

I. Bâtir une culture solide et pérenne de la sécurité de l'information

Le CHUSJ accorde une importance au respect du caractère confidentiel de l'information, de la vie privée, du secret professionnel, de la propriété intellectuelle et à la PRP. Le renforcement et le maintien d'une culture en matière de sécurité de l'information permettront de renforcer la confiance des différents acteurs à son égard. Le CHUSJ doit à cet effet établir des mesures garantissant :

- **La confidentialité des données :** afin d'empêcher tout accès non autorisé à l'environnement technologique du CHUSJ et aux informations qui s'y trouvent.
- **L'intégrité des données :** afin d'éviter toute altération non autorisée des informations du CHUSJ.
- **La disponibilité continue des données** : afin d'assurer que tout utilisateur légitime de l'environnement technologique du CHUSJ puisse accéder, s'il en a les droits, aux ressources informationnelles sans perturbation.

L'intégration de ces principes de sécurité de l'information dans tous les processus organisationnels et opérationnels du CHUSJ, incluant la gestion des projets et les relations avec les tiers, est essentielle. Cela signifie que les considérations de sécurité doivent être prises en compte dès la conception et la mise en œuvre de chaque processus et projets mais également lors des phases de contractualisation avec les tiers.

II. Définir les rôles et les responsabilités de chaque utilisateur

Garantir la sécurité de l'information et la PRP est une responsabilité partagée et commune à laquelle chaque utilisateur des actifs informationnels du CHUSJ doit être sensibilisé et formé. Cela

nécessite une attribution claire des rôles et des responsabilités à tous les niveaux de l'organisation, assurant ainsi une gestion sécurisée de l'information.

III. Se conformer aux normes et à la législation en vigueur

Le respect de toutes les réglementations, lois et normes pertinentes en matière de sécurité de l'information (normes sectorielles et technologiques) représente un engagement fondamental pour le CHUSJ. En honorant ses obligations légales, le CHUSJ développe par la même occasion des bonnes pratiques dans la gestion de ses actifs informationnels et renforce sa crédibilité et la confiance des différents acteurs à son égard.

IV. S'adapter aux évolutions

La présente politique doit être continuellement révisée de manière à apprécier les dernières évolutions technologiques, réglementaires, les menaces émergentes et les changements organisationnels au sein du CHUSJ.

4 Principes directeurs

Le CHUSJ reconnaît l'importance cruciale de protéger l'information et les technologies pour réaliser sa mission. Également, il revêt d'une importance capitale de superviser l'obsolescence et les risques liés aux équipements de génie biomédical en intégrant des clauses précises dans les appels d'offres avec les fournisseurs, assurant ainsi leur mise à jour régulière afin d'assurer la sécurité et la fiabilité de ces éléments essentiels.

Dans cet esprit, le CHUSJ souhaite adopter des solutions adéquates et conformes aux bonnes pratiques nationales et internationales. Les principes directeurs ci-dessous, basés sur les objectifs de la politique, représentent des exigences fondamentales intégrées dans la gouvernance, la gestion et les opérations du CHUSJ et qui s'appliquent à toute personne ou entité soumise à la politique.

4.1 Classifier les ressources informationnelles

Chaque ressource d'information est identifiée et classifiée à travers un processus d'évaluation partagé, permettant de déterminer sa criticité en termes de disponibilité, d'intégrité et de confidentialité.

Il convient de souligner que la classification prend en considération la valeur ou la criticité de l'actif pour les services de l'établissement. Cette méthodologie de classification constitue un pilier fondamental de notre engagement envers la sécurité de l'information.

Elle renforce notre capacité à identifier et à hiérarchiser les priorités en matière de protection des actifs critiques et également à allouer les ressources adéquates pour maintenir les niveaux de sécurité pour répondre aux exigences spécifiques de nos opérations.

4.2 Assurer une protection adaptée

Les mesures de protection sont ajustées en fonction de la criticité de l'actif informationnel et des risques associés, puis déployées tout au long du cycle de vie de l'information du CHUSJ, couvrant sa création, son enregistrement, son transfert, sa consultation, son traitement, son utilisation, sa transmission et sa conservation et archivage jusqu'à sa destruction. La criticité, la sensibilité de l'information, les risques, et par conséquent, les mesures de sécurité, peuvent varier durant ce cycle.

Le CHUSJ se réserve le droit de surveiller et d'effectuer des contrôles sur tout équipement informatique, matériel électronique ou tout autre support d'informations qu'ils contiennent, téléchargements, sites Internet visités, et, dans certaines circonstances, du courrier électronique, utilisant ou connecté aux actifs informationnels du CHUSJ.

Tout utilisateur doit être associé à un compte unique pour permettre le suivi de son activité à travers les systèmes d'information (ci-après le SI) du CHUSJ. Par conséquent, l'utilisation de comptes génériques est à éviter, bien que des exceptions puissent être autorisées par l'équipe de sécurité suivant l'analyse des besoins.

4.3 Organiser la gestion des environnements technologiques et leur maintenance

Seul le personnel autorisé par la Direction des ressources informationnelles, stratégies numériques et génie biomédical (ci-après DRISNGBM) peut assurer la maintenance des systèmes informatiques du CHUSJ, celle-ci s'effectue dans un environnement isolé de l'environnement de production. Les plages de maintenance des applications et des systèmes les supportant doivent être déterminées en collaboration avec les détenteurs d'actifs pour tenir compte des contraintes opérationnelles.

L'acquisition, le développement, et la maintenance des applications sont soumis à des processus formels contrôlés par la DRISNGBM.

Les SI critiques du CHUSJ ne sont accessibles que par des moyens sécurisés, dans un environnement contrôlé et restreint.

Les informations numériques, systèmes, procédures et documentation font l'objet d'une sauvegarde appropriée pour garantir disponibilité, intégrité et confidentialité, conformément aux critères établis.

Toute opération (création, modification ou suppression) sur les SI critiques doit être enregistrée dans des journaux d'événements sécurisés pour références futures.

Les ententes et contrats établis par le CHUSJ, notamment pour l'acquisition, le développement et la maintenance des applications et des équipements génie biomédical, intègrent des clauses assurant la conformité aux normes de sécurité de l'information du CHUSJ et sont sous la supervision directe de la DRISNGBM.

4.4 Opérer les actifs informationnels avec discernement et éthique

Le CHUSJ met à disposition des utilisateurs des actifs informationnels pour l'exercice de leurs fonctions. Ceci comprend, mais ne se limite pas, aux postes de travail, appareils mobiles de communication, applications et réseaux filaires et sans-fils corporatifs.

Il est impératif que chaque utilisateur les emploie de manière attentive, en respectant les lois et règlements en vigueur dans l'établissement. En aucun cas, ils ne doivent servir à la divulgation non autorisée d'informations confidentielles.

Si une telle situation se présente, l'utilisateur doit opter pour des moyens jugés sécuritaires et agir en conformité avec les prescriptions légales et éthiques. L'utilisateur doit également respecter les dispositions de la ***Procédure de gestion des incidents de confidentialité***. Le CHUSJ se réserve par ailleurs le droit de retirer l'accès à son réseau des appareils qui représentent un risque pour la sécurité informationnelle de l'établissement ou qui constituent une faille de sécurité potentielle.

4.5 Protéger les informations confidentielles et les renseignements personnels

Dans le cadre de sa mission le CHUSJ détient des données confidentielles, notamment des renseignements personnels, nécessitant la mise en place de mesures pour encadrer les risques associés à la divulgation non autorisée de ces informations (conformément au cadre législatif et aux lois applicables). Le CHUSJ doit notamment garantir que les renseignements personnels sont collectés de manière sécurisée, limités au strict nécessaire, exacts, à jour, complets, accessibles uniquement aux utilisateurs légitimes, traités avec discernement pour servir aux fins prévues ou autorisées par la loi et détruits ou anonymisés lorsque leur conservation n'est plus nécessaire selon le Calendrier de conservation du CHUSJ.

La sélection des mesures de sécurité repose sur l'analyse des risques impactant les informations. Plus précisément, la classification de l'information, l'évaluation des risques et l'établissement des exigences de sécurité doivent être effectués dès le début des travaux et persistés jusqu'à leur achèvement, afin de protéger l'information du CHUSJ durant tout son cycle de vie.

4.6 Maintenir l'intégrité, la valeur probante et la validité juridique de l'information

Préserver l'intégrité de l'information en fonction de la catégorisation, des besoins opérationnels, et des obligations légales et contractuelles est essentiel. Le CHUSJ doit particulièrement garantir la préservation de la valeur probante de l'information tout au long de son cycle de vie, indépendamment des changements de format ou de support, afin d'assurer sa validité juridique potentielle. Les processus et mécanismes de copie, classement, saisie, conservation, journalisation, transmission ou transfert de l'information doivent, par conséquent, assurer son intégrité et sa valeur probante.

4.7 Garantir la disponibilité et la préservation de l'information

Assurer l'accessibilité continue et la préservation de l'information est essentiel pour répondre aux besoins des personnes autorisées en temps opportun. Le CHUSJ, conformément au cadre législatif, doit mettre en place des mesures de planification, de contrôle, et de sécurité pour la création, l'utilisation, la conservation et la destruction des données, en se basant sur une catégorisation appropriée, en élaborant et maintenant à jour un calendrier de conservation et un plan de classification des données.

4.8 Préparer et anticiper la réponse aux incidents

En cas de violation de la sécurité informationnelle, le CHUSJ doit être en mesure de réagir rapidement et efficacement pour éviter des répercutions critiques sur ses activités. Des mécanismes de surveillance sont nécessaires pour suivre l'utilisation des systèmes et détecter toute anomalie.

Lors de situations exceptionnelles mettant à risque la sécurité informationnelle du CHUSJ, des actions restrictives pourront être mises en place au niveau des actifs impactés afin de limiter la propagation au reste des SI du CHUSJ. Les détenteurs d'actifs informationnels ainsi que les gestionnaires sont sensibilisés aux attentes en matière de sécurité de l'information, notamment concernant les procédures de collaboration nécessaires lors de situations urgentes et/ou critiques, à travers un plan de réponse prévu lors d'incidents de cybersécurité.

Enfin, le CHUSJ en sa qualité d'organisme public, collabore à la fois avec des instances provinciales (portefeuille Ministériel) et gouvernementales, afin d'organiser la gouvernance de la sécurité de l'information et les opérations qui y sont liées (dont la réponse aux incidents de cybersécurité), et ce, telles que le prévoient les dispositions décrites dans le *cadre de gestion gouvernemental et provincial pour la sécurité de l'information MSSS-CDG01* (voir section Cadre de gouvernance de la sécurité de l'information, Gouvernance ministérielle et gouvernementale).

4.9 Permettre la continuité des services de soins et des opérations

Le CHUSJ élabore un plan de continuité des activités (ci-après PCA) pour les actifs assurant la continuité de services importants et critiques de l'établissement. Le PCA vise à fournir des procédures tactiques et opérationnelles pour assurer la continuité des activités et des services en cas d'indisponibilité des actifs informationnels.

Par ailleurs, la responsabilité de définir, de maintenir, d'améliorer et de diffuser les PCA aux parties prenantes incombe aux détenteurs des actifs concernés.

4.10 Mettre en place des plans de relève informatique

Le Chef de la sécurité organisationnelle (ci-après CSIO) assure la mise en place, des plans de relève informatique (ci-après PRI). Ces PRI visent à assurer la reprise des opérations des SI critiques aux activités des services associés, dans un délai raisonnable en cas de panne majeure.

De plus pour être efficace et résilient il est important de planifier des tests et des révisions des mesures de relève, que ce soit lors d'importantes acquisitions impactant les ressources informationnelles ou lors de changements organisationnels.

4.11 Formaliser un processus de gestion des accès et des identités (GIA)

Les utilisateurs autorisés à accéder à l'information jouent un rôle crucial dans la sécurité de l'information. Ainsi, l'accès à l'information et aux actifs informationnels est soumis à l'obtention d'une autorisation formelle, conditionnée par des vérifications, notamment sur l'identité des personnes auxquelles sont attribués les privilèges et les autorisations accordées. Ces privilèges varient en fonction de la nature ou de la sensibilité de l'information à laquelle une personne a accès et ne doivent servir qu'aux fins prévues.

4.12 Encadrer l'utilisation des appareils et outils personnels

Dans le respect des dispositions en vigueur dans l'établissement, notamment en matière de protection des renseignements personnels, sans toutefois s'y limiter, il est strictement interdit de télécharger ou d'archiver localement, sur un appareil ou outil personnel, des données de nature sensibles et confidentielles appartenant ou détenues par le CHUSJ.

De plus, tout appareil personnel ayant accès aux ressources informationnelles du CHUSJ doit être sécuritaire. Le CHUSJ se réserve le droit de retirer les accès au réseau informatique à tout appareil présentant un risque pour l'organisation.

4.13 S'assurer de l'utilisation vigilante des nouvelles technologies et des services de stockage de données accessible sur le web

Bien que l'innovation et la poursuite des améliorations soient encouragées, le CHUSJ reconnaît également l'importance de la vigilance face aux nouvelles technologies émergentes, notamment les outils d'intelligence artificielle (IA) générative (ex : ChatGPT), et promeut une utilisation responsable et éthique de ces innovations.

De même, l'utilisation à usage professionnel des espaces de stockage partagés sur le web autre que les espaces autorisés par le CHUSJ et le MSSS, tels que Dropbox, doit être évitée, afin de garantir la sécurité et la confidentialité des informations du CHUSJ.

Le CHUSJ encadrera l'usage des technologies mentionnées ci-dessus à travers des procédures et des directives, et il sera impératif pour les utilisateurs de les suivre et s'y conformer pour garantir la sécurité et l'intégrité de nos systèmes.

Tout manque de discernement dans l'emploi de telles technologies, quelle qu'en soit la cause, peut entrainer des sanctions disciplinaires telles qu'elles sont décrites dans la section associée de cette politique.

4.14 Encadrer le travail à distance

Les accès distants aux services et logiciels nécessaires sont réservés aux personnes autorisées par leur gestionnaire, conformément aux modalités définies par l'équipe de sécurité du CHUSJ et dans le respect des termes des conventions collectives. Les personnes autorisées doivent se conformer aux ententes formelles et aux directives établies pour respecter la politique en vigueur. En particulier, les personnes autorisées à effectuer du travail à distance doivent régulièrement se présenter physiquement sur le site du CHUSJ afin d'éviter toute désynchronisation des appareils avec le réseau informatique du CHUSJ.

En plus, pour les personnes nécessitant de travailler à l'étranger, que ce soit dans le cadre d'un déplacement professionnel ou pour des fonctions telles que des congrès ou des colloques, une demande de modification du jeton d'accès à distance doit être effectuée via Octopus. Cela permettra de garantir que seules les personnes légitimes et autorisées puissent accéder aux ressources à distance, tout en assurant la sécurité et la conformité avec nos politiques internes.

4.15 Auditer les Systèmes d'Information

Le CHUSJ utilise des outils de surveillance et de contrôle pour enregistrer l'utilisation de ses actifs, permettant une analyse continue de leur utilisation. Dans le but de détecter les logiciels

malveillants, le CHUSJ surveille l'ensemble du trafic sur ses réseaux informatiques, y compris les connexions chiffrées, tout en respectant les lois applicables. À des fins de sécurité, le CHUSJ se réserve le droit d'auditer de manière éthique et responsable les services collaboratifs mis à disposition de ses effectifs (ex : courriels en ligne, messagerie professionnelle, etc.) sans en violer la vie privée. Seuls les sites jugés de confiance absolue peuvent être exclus de ces audits.

4.16 Former et sensibiliser

Le CHUSJ s'engage à faire bénéficier ses effectifs de formations visant notamment à les sensibiliser et les responsabiliser en matière de sécurité de l'information. L'objectif est de permettre à chaque individu de comprendre pleinement son rôle et ses obligations en la matière, mais aussi de veiller à ce que chacun soit au courant des dernières menaces émergentes afin d'adopter une réaction adéquate. Le tout doit venir consolider et favoriser une culture solide axée sur la sécurité informationnelle.

4.17 Respecter la propriété intellectuelle

Le CHUSJ se conforme aux exigences légales en matière de propriété intellectuelle liées à l'utilisation de produits, documents, informations et brevets. Chaque utilisateur est tenu de respecter ces exigences, qu'il s'agisse de droits de propriété intellectuelle détenus par le CHUSJ ou par d'autres entités, telles que sa fondation.

4.18 Viser l'amélioration continue

L'amélioration continue et la saine gestion du changement sont au cœur de l'approche de la sécurité de l'information du CHUSJ. Les menaces, les vulnérabilités et les risques évoluent constamment, tout comme les technologies et les meilleures pratiques en matière de sécurité. Par conséquent, le CHUSJ s'engage à examiner l'architecture, la configuration des composants réseaux et la configuration des actifs critiques.

5 Cadre législatif

Cette politique s'intègre dans le cadre législatif québécois établi par le Ministère de la Cybersécurité et du Numérique (MCN) et dans le cadre normatif constitué par les politiques de sécurité de l'information du Ministère de la Santé et des Services Sociaux (MSSS) et respecte les normes et standards de sécurité internationales.

La liste exhaustive des cadres législatif et normatif applicables est fournie en **annexe**.

6 Définitions

Les différentes définitions des terminologies ci-après font partie de la présente politique et sont indiquées au niveau de l'**annexe**.

7 Règles d'application

La présente politique s'applique à l'ensemble des utilisateurs de l'information au sein du CHUSJ, englobant les dirigeants, le personnel de tous statuts, et toute personne physique agissant en tant que patient, consultant, médecin, chercheur, partenaire, fournisseur ou visiteur ayant accès aux actifs informationnels du CHUSJ. Elle inclut également toute personne dûment autorisée à accéder à ces informations, et s'applique notamment par extension à la Fondation Sainte-Justine.

Les informations visées par cette politique englobent celles détenues par le CHUSJ dans le cadre de sa mission, qu'elles soient conservées en interne ou par des tiers, et concernent des formats tant numériques que non numériques.

Les activités concernées par cette politique englobent toutes celles qui impliquent l'utilisation, la transmission ou la conservation, sous quelque forme que ce soit, d'un actif informationnel appartenant ou détenu par le CHUSJ, sans égard aux supports ou aux emplacements, qu'elle soit exercée dans les locaux de cette dernière, ou un autre lieu, tout au long du cycle de vie de l'actif.

8 Rôles et responsabilités

Chaque niveau de l'organisation contribue à la sécurité de l'information Notre ambition est de souligner l'importance du leadership, de la collaboration et de l'intégration pour créer une culture de sécurité informationnelle robuste, qui soit basée sur les risques et notre capacité à les gérer de la manière la plus efficace.

8.1 Conseil d'administration

Le conseil d'administration approuve la présente politique générale de sécurité de l'information du CHUSJ, laquelle est conforme à la Politique provinciale de sécurité de l'information et au Cadre de gestion de la sécurité de l'information adoptés par le MSSS et suit leur application dans le CHUSJ.

De plus le conseil d'administration reçoit et entérine annuellement ou au besoin le Bilan de sécurité de l'information du CHUSJ.

8.2 Direction Générale

La Direction générale du CHUSJ est chargée de :

- ✓ Fournir un soutien financier et organisationnel ;
- ✓ Promouvoir une culture de sécurité robuste;
- ✓ Montrer l'exemple en matière de conformité;
- ✓ Approuver les initiatives de sécurité informationnelle;
- ✓ Déterminer les mesures visant à favoriser l'application de la présente politique ainsi que le respect des lois et règles en matière de sécurité de l'information.

- ✓ Convenir des orientations stratégiques et des plans d'action;
- ✓ Superviser les bilans de sécurité de l'information, et approuver les directives, processus, et procédures soutenant l'application de cette politique;
- ✓ Participer de manière proactive à la structure de la gouvernance de la sécurité de l'établissement.

8.3 Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO est le responsable de la prise en charge globale de la sécurité de l'information au sein du CHUSJ, à ce titre il/elle :

- ✓ Formule des recommandations et fixe les objectifs concernant les besoins d'audit de sécurité, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information et la mise à jour du Cadre normatif de sécurité de l'information du CHUSJ ;
- ✓ S'assure que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires comprennent des clauses garantissant le respect des exigences de sécurité de l'information;
- ✓ Garantit la coordination et la cohérence des actions menées au sein du CHUSJ en matière de sécurité de l'information, notamment en conseillant les détenteurs d'actifs informationnels dans les unités même en dehors des heures ouvrables;
- ✓ Supervise ses équipes dans la réalisation des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information;
- ✓ Veille à la mise en place d'un processus de gestion des incidents, des menaces et des vulnérabilités pour l'organisation conformément aux directives du MSSS et collaboration avec ses instances;
- ✓ Contribue aux analyses de risques de sécurité et institutionnelles de l'information afin d'identifier les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées.

8.4 Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) du CHUSJ a pour mission principale de coordonner la mise en œuvre de la politique de sécurité de l'information au sein de son organisation. À ce titre il/elle a la charge de :

- ✓ Participer aux audits et analyses de risques de sécurité de l'information afin d'identifier les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;

- ✓ Élaborer et tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications;
- ✓ Collaborer étroitement avec la personne CSIO en lui apportant le soutien technique nécessaire à l'exercice de ses responsabilités;
- ✓ Maintenir une veille continue sur les risques, les menaces et les vulnérabilités;
- ✓ Contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information du CHUSJ;
- ✓ Tenir à jour le registre des incidents ayant pu mettre en péril la sécurité de l'information, de documenter ces incidents et d'en tenir informé la personne CSIO;
- ✓ Assurer la coordination de l'équipe de réponse aux incidents de sécurité de l'information et mettre en œuvre les stratégies appropriées;
- ✓ Contribuer aux audits et évaluations de risques et de conformité pour identifier les risques et les non-conformités;
- ✓ Suivre et participer au partage et recueil d'information de la communauté de sécurité de l'information pour le compte du CHUSJ;
- ✓ Communiquer avec les instances ministérielles et gouvernementales pour coordonner les actions de sécurité informationnelle.

8.5 Responsables de la protection des renseignements personnels (RPRP)

Sous la supervision de la Direction Qualité, Évaluation, Performance et Éthique, les Responsables de la protection des renseignements personnels jouent un rôle essentiel dans le développement et la mise en œuvre de pratiques qui respectent les normes en vigueur conformément aux responsabilités qui leur sont attribuées dans la *Politique de gouvernance des renseignements personnels*.

Par ailleurs, le CHUSJ procède à une Évaluation des Facteurs relatifs à la Vie Privée (EFVP) en vertu de la LADPRP (*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*) lors de projets d'acquisition, de développement et de refonte de système d'information impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Cette évaluation est réalisée conjointement avec les équipes de sécurité de l'information concernant les projets qui concernent, entre autres, des bases de données et des logiciels d'application.

8.6 Équipes opérationnelles de maintien de la sécurité informationnelle

Les équipes opérationnelles assurent le maintien de la sécurité informationnelle des actifs du CHUSJ, notamment en fournissant des services de support informatique puis en traitant les demandes et les incidents. Au sein de ces équipes on retrouve :

8.6.1 Le Centre de service de la direction des technologies (CSDT)

Le Centre de Services de la Direction des Technologies (CSDT) est au cœur de la prestation de services informatiques au sein du CHUSJ. Il assure un support technique aux utilisateurs, gérant les incidents signalés et répondant aux demandes de service. Le CSDT s'engage dans la gestion des changements, la maintenance préventive, la formation des utilisateurs, la surveillance des performances des systèmes, et contribue à la sécurité de l'information. En collaborant avec d'autres services, le CSDT favorise une intégration harmonieuse des processus et s'implique dans des initiatives d'amélioration continue pour optimiser les opérations informatiques du CHUSJ.

8.6.2 Le Centre des opérations de sécurité (COS ou SOC)

Le Centre des Opérations de Sécurité (SOC) est un pilier central de la posture de cybersécurité du CHUSJ. Il surveille constamment les activités informatiques, détecte les menaces potentielles, et coordonne des actions immédiates en cas d'incident. Les responsabilités du SOC incluent l'analyse des événements de sécurité, la gestion des alertes, la collaboration avec d'autres équipes, la veille technologique, la formation du personnel, et la génération de rapports périodiques pour la direction. En s'appuyant sur une démarche d'amélioration continue, le SOC joue un rôle crucial dans la détection précoce, la réponse rapide et la gestion proactive des menaces informatiques.

8.7 Détenteurs de l'information

Le détenteur de l'information est un collaborateur du CHUSJ responsable du système d'information, de sa bonne utilisation, de son évolution, de l'information qu'il contient, de la qualité des données ainsi que de l'habilitation des pilotes (expertise et couverture). Il :

- ✓ Participe à l'ensemble des activités relatives à la sécurité pour son système;
- ✓ Autorise les droits d'accès aux informations incluant les systèmes d'information dont il est détenteur;
- ✓ S'assure que les mesures de sécurité appropriées soient élaborées, approuvées, mises en place et appliquées systématiquement puis s'assure que les actifs dont il assume la responsabilité soient consignés;
- ✓ Autorise les correctifs nécessaires, les modifications demandées et les nouvelles versions de l'application puis s'assure que les changements soient faits de manière sécuritaire;
- ✓ S'assure que le système sous sa responsabilité soit maintenu à jour et que les plages de maintenances soient prévues à cet effet;
- ✓ S'assure de l'intégrité et la sauvegarde des données;
- ✓ Effectue l'évaluation des risques à la sécurité de l'information avec l'aide du conseiller à la sécurité de l'information;
- ✓ Est responsable d'avoir un plan de continuité pour son système d'information.

8.8 Gestionnaires (incluant les chefs de service)

L'intégration de la sécurité assure que les mesures adéquates soient prises en compte dès l'initiation des projets et dans les opérations quotidiennes du CHUSJ. Les gestionnaires sont responsables d'assurer cette intégration dans leurs activités courantes et veillent à ce que tous les effectifs sous leur charge connaissent et respectent leurs obligations découlant de la présente politique. En particulier, ils doivent les informer précisément des normes, des directives et des procédures de sécurité en vigueur, mais aussi les sensibiliser à l'importance des enjeux de sécurité. De plus les gestionnaires doivent communiquer au CSIO tout problème d'incidence majeure pour la sécurité de l'information.

8.9 Pilotes de systèmes et d'applications

Conformément à la ***Politique de pilotage des systèmes d'information***, les pilotes d'application jouent un rôle essentiel en garantissant une gestion optimale des actifs sous leur responsabilité dès leur mise en exploitation, assurant ainsi le bon fonctionnement et la sécurité des systèmes qu'ils supervisent. Ils veillent à ce que l'attribution des droits d'accès, leur gestion et leur révocation soient appliqués conformément aux règles de sécurité du CHUSJ. Les pilotes de systèmes doivent également co-définir avec les responsables des services concernés, des plages de maintenance des systèmes dont ils ont la charge et veiller à appliquer les mises à jour et correctifs de sécurité adéquats.

En outre, les pilotes sont tenus d'initier l'exercice de mise à jour des plans de continuité des activités (PCA) pour garantir une réponse efficace en cas d'incidents ou de situations critiques, assurant ainsi la résilience et la continuité opérationnelle des systèmes.

8.10 La Direction des ressources financières et de la logistique (DRFL)

La DRFL a la responsabilité de s'assurer, par des mesures contractuelles, que l'ensemble des fournisseurs veillent à la protection de l'information tout au long du cycle de vie du contrat et au respect des exigences de sécurité du CHUSJ.

Elle s'assure que les fournisseurs du CHUSJ se conforment aux mesures de sécurité en place afin de protéger les actifs informationnels, quel qu'en soit le support.

8.11 La Direction qualité, évaluation, performance et éthique (DQEPE)

La DQEPE est responsable de collaborer avec le CSIO pour l'identification et la mise en place d'indicateurs de suivis des orientations en matière de sécurité pour la haute direction. Elle s'assure aussi que les incidents de sécurité ayant un risque clinique majeur soient consignés dans les registres appropriés.

Également, elle participe aux projets d'envergure, selon les priorités de l'organisation en fournissant les ressources spécialisées : en éthique, gestion de projets ou ayant les compétences

requises pour la mise en œuvre d'orientations stratégiques en matière de sécurité de l'information.

8.12 Utilisateurs

Toute personne visée par la politique, a l'obligation de la respecter afin de protéger l'information mise à sa disposition par le CHUSJ et de signaler tout incident de sécurité à l'équipe opérationnelle de la sécurité par l'intermédiaire de la billetterie mise en place au CSDT. Par ailleurs, tout incident de confidentialité doit être déclaré conformément à la ***Procédure de gestion des incidents de confidentialité***.

9 Cadre de gouvernance de la sécurité de l'information

9.1 Comité stratégique de la sécurité de l'information

Le Comité Stratégique de la Sécurité de l'Information (ci-après CSSI) occupe une position cruciale au sein de l'organisation en guidant les décisions stratégiques liées à la sécurité de l'information. Composé de hauts dirigeants et de cadres supérieurs, le CSSI se concentre sur l'élaboration des grandes orientations stratégiques, l'approbation des politiques de sécurité de l'information et l'allocation des ressources nécessaires. Ce comité joue un rôle clé dans l'alignement de la sécurité de l'information sur les objectifs globaux du CHUSJ. En se réunissant de manière périodique, le CSSI évalue les risques majeurs, approuve des directives stratégiques et veille à ce que la sécurité de l'information soit intégrée de manière cohérente dans la vision globale du CHUSJ.

9.2 Comité tactique de la sécurité de l'information

Le Comité Tactique de la Sécurité de l'Information (CTSI) se consacre à la mise en œuvre opérationnelle des politiques et des mesures de sécurité établies par le CSSI. Composé de membres des équipes opérationnelles de sécurité, de responsables de secteurs d'activités impliqués dans la gestion quotidienne de la sécurité, et de représentants techniques, le CTSI coordonne les activités concrètes nécessaires pour assurer la sécurité des informations. Réunissant régulièrement des experts opérationnels, le CTSI résout des problèmes spécifiques, surveille les indicateurs de performance, et s'assure que les politiques de sécurité sont mises en œuvre de manière efficace à tous les niveaux de l'organisation. Ce comité assure la liaison entre la vision stratégique du CSSI et les actions concrètes nécessaires pour garantir la protection des actifs informationnels de l'organisation.

9.3 Tables de travail

Les tables de travail sont des sous unités du comité tactique de la sécurité de l'information du CHUSJ chargées de définir les mesures opérationnelles à mettre en place au niveau des périmètres

concernés afin de contribuer au renforcement de la sécurité de l'information. Au sein du CHUSJ on distingue quatre tables de travail :

- **Sécurité physique**

Table de travail dédiée à garantir la mise en place de mesures garantissant la sécurité physique des appareils et équipements supportant l'information sensible du CHUSJ.

- **Sensibilisation à la sécurité**

Table de travail dédiée aux campagnes et activités de sensibilisation des effectifs à la sécurité de l'information.

- **Sécurité système d'information**

Table de travail dédiée à l'audit, la maintenance et le durcissement des systèmes supportant l'information du CHUSJ.

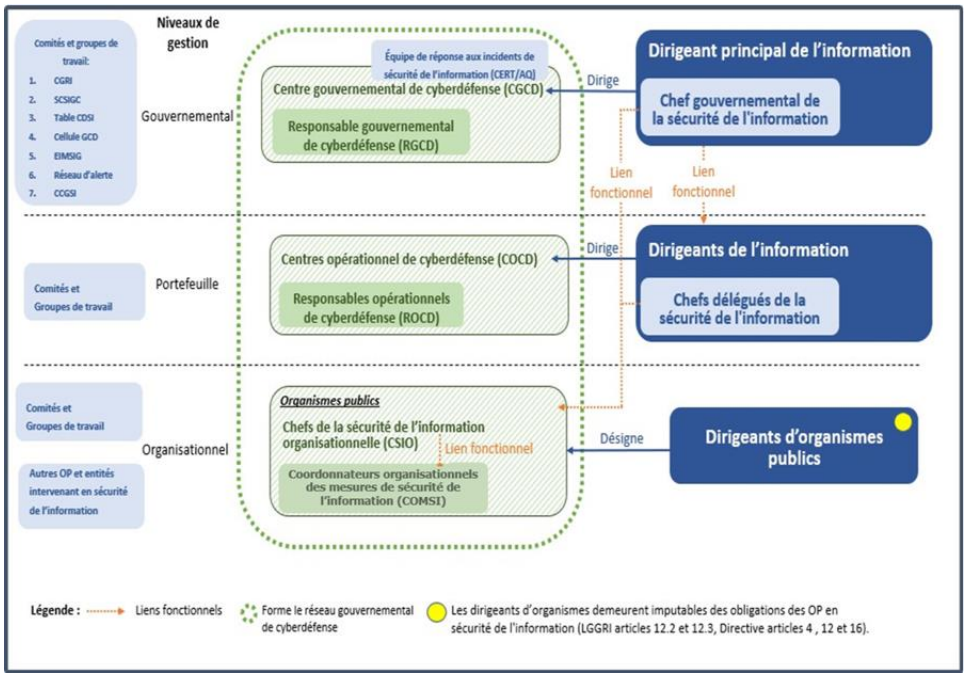
- **Sécurité de l'infrastructure**

Table dédiée à la mise en place de mesures assurant la sécurité des infrastructures supportant les actifs informationnels du CHUSJ.

9.4 Gouvernance ministérielle et gouvernementale

Le CHUSJ, en qualité d'organisme public, collabore avec des intervenants du réseau de la santé et des services sociaux (ci-après RSSS) dont les rôles, responsabilités et les modalités de contribution sont précisément décrites dans le cadre provincial de gestion de la sécurité de l'information (MSSS-CDG01), dans le respect des cinq principes directeurs préconisés par la Directive gouvernementale sur la sécurité de l'information : l'éthique, l'évolution, la responsabilité-imputabilité, la transparence et l'universalité.

- **Structure de gouvernance de la sécurité de l'information gouvernementale**



Source : Cadre gouvernemental de gestion de la sécurité de l'information

9.4.1 Le centre opérationnel de cyberdéfense (COCD)

Le COCD opère sous la direction et la coordination du Chef délégué de la sécurité de l'information (CDSI), qui nomme un responsable opérationnel de cyberdéfense (ROCD) pour le soutenir. Sa mission consiste à assurer le commandement, la coordination, l'amélioration continue et le leadership en matière de cybersécurité pour le MSSS et les établissements publics, intervenant à un niveau tactique et opérationnel. Parmi ses responsabilités figurent la gestion rapide des événements de sécurité en collaboration avec les répondants identifiés, la réalisation régulière de vérifications de sécurité des systèmes, la définition de mécanismes de suivi et de concertation, le soutien à la mise en place et à l'évolution d'un centre des opérations de sécurité (ou SOC), le maintien d'une offre de services de cyberdéfense, la dispensation d'avis et de conseils, la formulation de recommandations pour renforcer la sécurité, et l'exécution d'autres activités de SI assignées par le CDSI.

9.4.2 Le centre gouvernemental de cyberdéfense (CGCD)

Le CGCD joue un rôle central en tant que centre de commandement des opérations de cyberdéfense et centre de coordination et de soutien pour les membres du RSSS. Il a pour mission d'améliorer continuellement le Réseau en développant des pratiques et des expertises. Opérant au niveau tactique et opérationnel, le CGCD est chargé d'offrir des services centralisés en sécurité de l'information, de surveiller constamment les cybermenaces et de coordonner des interventions rapides en cas d'incidents de sécurité potentiellement préjudiciables aux données numériques gouvernementales québécoises. Ses responsabilités comprennent la gestion concertée des menaces, vulnérabilités et incidents, l'optimisation des ressources pour l'analyse des risques à

l'échelle gouvernementale, la surveillance continue des systèmes gouvernementaux, la recommandation de correctifs de sécurité, la définition de mécanismes de suivi et de concertation, le développement et le maintien de l'expertise en cybersécurité, la dispensation d'avis et de conseils, la création d'outils partageables, le développement de services de sécurité, et la mise en relation des intervenants de sécurité au sein de l'administration publique et avec d'autres partenaires pertinents.

10 Dispositions finales

10.1 Mesures disciplinaires et sanctions

Toute personne enfreignant cette politique ainsi que les règles et directives associées s'expose à des mesures administratives, disciplinaires ou légales. Ces mesures seront équitables, raisonnables et proportionnées à la sévérité et aux impacts des actions commises. Elles seront appliquées conformément aux dispositions établies dans les lois du travail, les conventions collectives, les accords définissant les conditions de travail des employés non syndiqués, les contrats individuels de travail, les contrats de service ou tout autre document réglementaire ou législatif pertinent.

10.2 Processus de Révision

Les révisions de la politique seront entreprises par le CSIO en consultation avec les parties concernées, y compris la direction, le responsable de la sécurité des infrastructures et d'autres experts internes ou externes. La révision doit permettre d'évaluer la pertinence continue de la politique par rapport aux objectifs du CHUSJ et aux nouvelles réalités de la sécurité de l'information. Les changements internes et externes doivent être pris en compte. De plus, les bilans des différents incidents et les nouvelles connaissances acquises doivent permettre d'identifier des axes et des opportunités d'amélioration.

10.3 Communication des Révisions

Les modifications apportées à la politique seront communiquées à l'ensemble du personnel et, si nécessaire, à d'autres parties prenantes, selon les processus en place pour la révision des politiques afin d'assurer une compréhension claire des changements et encourager leur adhésion.

10.4 Adoption des Mises à jour

Tous les membres du personnel sont tenus de respecter les mises à jour de la politique après son entrée en vigueur. La non-conformité aux nouvelles dispositions peut entraîner des mesures correctives.

Numéro RPP : 2024-A-058-r0	
Approbation d'entrée en vigueur par le : Gestionnaire ou directeur : N/A Comité de direction : 2024-02-27 Comité de régie : N/A Conseil d'administration : N/A Résolution no : N/A	*Contenu révisé et approuvé le :* Gestionnaire ou directeur : N/A Comité de direction : N/A Comité de régie : N/A Conseil d'administration : N/A Résolution no : N/A

11 Instances consultées

Au CHUSJ :	À l'externe :
Direction qualité, évaluation, performance et éthique	Gartner Inc. (entreprise de conseil et de recherche)
Centre de recherche du CHU Sainte-Justine	Sia Partners (Cabinet de conseil et de gestion)
Direction des personnes, de la culture, du leadership, des communications et des relations publiques	
Direction des services professionnels	

12 Références

DOCUMENT DISPONIBLE DANS L'INTRANET DU CHUSJ

- CHU Ste-Justine, 2024, ***Procédure de gestion des incidents de confidentialité***. https://intranet.chusj.org/fr/References/Reglements-politiques-procedures/Tous
- CHU Ste-Justine, 2024, ***Politique de pilotage des systèmes d'information***. https://intranet.chusj.org/fr/References/Reglements-politiques-procedures/Tous

13 Annexes

13.1 Cadre normatif et légal

1- Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI);

2- La Directive gouvernementale sur la sécurité de l'information (2021);

3- Le Cadre gouvernemental de gestion de la sécurité de l'information;

4- Le cadre provincial de gestion de la sécurité de l'information (MSSS-CDG01);

5- La politique provinciale sur la sécurité de l'information (MSSS-POL01);

6- La Directive sur la Cybersécurité (MSSS-DIR03) ;

7- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1 (LADPRP) ainsi que les règlements qui en découlent;

8- MSSS-DIR04 – Directive sur l'utilisation sécuritaire des outils collaboration

9- Termes et condition des outils collaboratifs du MSSS

10- La norme NIST (National Institute of Standards and Technology) qui liste les bonnes pratiques pour la gestion les risques liés à la cybersécurité;

11- La norme ISO 27001/27002 qui établit les normes de mise en œuvre d'un système de management de la sécurité de l'information et des contrôles de sécurité.

13.2 Définitions

Actif informationnel : Actif composé ou supportant de l'information. Cela inclut les connaissances, les données ainsi que les documents et les supports tangibles ou intangibles (ex. : papier, matériel, logiciel, réseau, personne) permettant son traitement, son exploitation, sa transmission ou sa conservation aux fins d'utilisation prévue.

Numéro RPP : 2024-A-058-r0	
Approbation d'entrée en vigueur par le : Gestionnaire ou directeur : N/A Comité de direction : 2024-02-27 Comité de régie : N/A Conseil d'administration : N/A Résolution no : N/A	*Contenu révisé et approuvé le :* Gestionnaire ou directeur : N/A Comité de direction : N/A Comité de régie : N/A Conseil d'administration : N/A Résolution no : N/A

Comité sur l'accès à l'information et la protection des renseignements personnels (CAIPRP) : comité formé en vertu de la *Politique de gouvernance des renseignements personnels* et chargé de soutenir le CHUSJ dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la LADPRP (aussi appelé « CAIPRP »).

Confidentialité : Propriété d'une information de n'être accessible ou divulguée qu'aux personnes ou entités désignées et autorisées, selon des critères établis dans les lois applicables, et qui doit être protégée par un moyen approprié, lors de sa transmission, son utilisation et sa conservation.

Conservation des renseignements personnels : Action de détenir des renseignements personnels, peu importe le support, que ces renseignements soient activement utilisés ou non. Le CHUSJ détient les renseignements personnels même lorsqu'il confie la conservation à un tiers.

Cybersécurité : La cybersécurité est un ensemble de pratiques, de politiques, de technologies et de mesures visant à protéger les systèmes informatiques, les réseaux, les données et les informations contre les menaces, les attaques et les vulnérabilités. L'objectif de la cybersécurité est d'assurer la confidentialité, l'intégrité et la disponibilité des actifs informationnels tout en minimisant les risques liés à la cybercriminalité, à la perte de données et aux interruptions de service.

Cycle de vie des renseignements personnels : Ensemble des étapes visant le traitement d'un renseignement personnel soit la collecte, l'utilisation, la communication, la conservation et la destruction ou l'anonymisation de celui-ci.

Destruction des renseignements personnels : Action de détruire, de façon permanente et irréversible, un renseignement personnel, mettant ainsi fin au cycle de vie de celui-ci.

Disponibilité : Caractéristique d'une ressource informatique garantissant qu'elle est accessible et utilisable en temps voulu par les utilisateurs autorisés, sans interruption ni altération non autorisée.

Donnée sensible ou confidentielle : Donnée en raison de sa nature, de sa valeur ou de son importance stratégique pour l'organisation, est désignée comme devant être traitée avec le plus haut niveau de confidentialité et de protection. Ces données sont généralement identifiées comme telles en raison de leur potentiel à causer des préjudices significatifs en cas de divulgation, d'accès non autorisé ou d'utilisation inappropriée.

Environnement informatique : Ensemble des composantes matérielles et logicielles, de la structure organisationnelle et des politiques et procédures de contrôle qui constituent le cadre d'exploitation d'un système informatique.

Gouvernance de l'information : Stratégie, cadre interdisciplinaire composé de normes, processus, rôles et mesures qui tiennent les organisations et les individus responsables du bon traitement des actifs informationnels.

Information : Ensemble de données, de renseignements, peu importe le support, intelligibles sous forme de mots, de sons ou d'images, incluant des renseignements personnels, consignés ou détenus par le CHUSJ, y compris une information provenant d'un tiers, dont la structure et le contexte permettent de véhiculer un sens, et donc susceptible d'informer la personne à qui elle est transmise et de générer des connaissances.

Infrastructure : Ensemble de toutes les ressources technologiques sur lesquelles reposent l'organisation et la communication de l'information à l'intérieur d'une entreprise, d'un organisme, d'un territoire ou d'un pays.

Intégrité : Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation.

Projet (ou projet en ressources informationnelles) : Fait référence à un ensemble d'actions menant au développement, à l'acquisition, à l'évolution ou au remplacement d'un actif informationnel ou d'un service en ressources informationnelles et ce, indépendamment du mode de stockage des données et de leur traitement (stockage et traitement interne, externalisation, infonuagique, etc.).

Évaluation des facteurs relatifs à la vie privée (EFVP) : Démarche préventive visant à mieux protéger les renseignements personnels et à respecter la vie privée des personnes physiques en considérant tous les facteurs d'un projet qui auront un impact positif ou négatif sur le respect de la vie privée et la protection des renseignements personnels des personnes concernées, notamment :

- la conformité d'un projet à la législation applicable et le respect des principes qui l'appuient;
- l'identification des risques d'atteinte à la vie privée engendrés par un projet et l'évaluation de leurs impacts;
- la mise en place de stratégies pour éviter ces risques ou les réduire efficacement;
- l'évaluation des bénéfices découlant du projet.

Renseignement personnel : Renseignements qui concernent une personne physique et permettant, directement ou indirectement, de l'identifier.

Protection des renseignements personnels (PRP) : La PRP vise à garantir la confidentialité et la sécurité des renseignements personnels des individus, conformément aux lois et normes établissant les droits des personnes et les obligations des organisations en matière de renseignements personnels. Son objectif principal est de préserver la vie privée des individus.

Sécurité de l'information : Assurance, par un ensemble de mesures de sécurité, de l'atteinte des objectifs de disponibilité et de protection, de l'intégrité et de la confidentialité de l'information durant son traitement et sa conservation, ainsi que de l'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'ils posent.

Système informatique : Ensemble composé d'un ou de plusieurs ordinateurs en réseau, des périphériques, du logiciel d'exploitation, des logiciels d'application et des installations de réseau, coordonné de manière à permettre le traitement et l'échange d'informations.

Utilisation Sécuritaire des Actifs Informationnels : Se réfère à l'ensemble des pratiques et des comportements adoptés par les utilisateurs, les employés et les parties prenantes d'une organisation pour garantir que les informations et les données sont traitées, stockées et partagées de manière à minimiser les risques de perte, de divulgation non autorisée ou de compromission. Cela inclut le respect des politiques de sécurité, la protection des identifiants et des mots de passe, la gestion des accès, la sensibilisation à la sécurité, la sauvegarde régulière des données et le respect des normes de sécurité établies par l'organisation.