Politique de Sécurité du Système d'Information (PSSI)
Projet Hospitalier

Kenzi BOUGHADOU

Hugo GRILLET

Table des matières

1. Objectifs et portée de la PSSI

La présente Politique de Sécurité du Système d'Information (PSSI) constitue un document stratégique essentiel. Elle définit les règles fondamentales visant à assurer la protection, le contrôle et la gestion sécurisée des données informatiques indispensables à la réalisation des missions de soins au sein de l'établissement hospitalier.

La PSSI a pour finalité première de garantir en permanence :

- La disponibilité des systèmes et des informations, afin d'assurer la continuité et l'efficacité des soins,
- L'intégrité des données traitées, pour garantir l'exactitude, la cohérence et la fiabilité de l'information,
- L'imputabilité des actions réalisées, en assurant la traçabilité et la responsabilité individuelle sur les systèmes,
- La confidentialité des données, en particulier celles à caractère personnel et médical, conformément aux obligations légales et éthiques.

Portée :

La PSSI s'impose à tous les acteurs intervenant dans le cadre de l'utilisation du Système d'Information de l'établissement, sans distinction :

- Utilisateurs internes (agents titulaires, contractuels, praticiens hospitaliers, chercheurs, etc.),
- Utilisateurs externes (prestataires de services, fournisseurs, partenaires institutionnels, etc.),
- Utilisateurs permanents ou temporaires, autorisés à accéder aux ressources numériques.

La PSSI couvre de manière exhaustive :

- Tous les actifs informationnels, incluant les documents administratifs et médicaux, bases de données, applications métiers, logiciels spécialisés, et toute information traitée dans le cadre des missions hospitalières,
- L'ensemble des équipements informatiques (serveurs, postes de travail fixes et portables, dispositifs mobiles, objets connectés, équipements de télécommunication, etc.) utilisés pour stocker, transmettre ou traiter des données informatiques,
- Tous les moyens de communication numériques internes et externes, assurant le flux d'informations au sein de l'établissement.

2. Contexte et enjeux

Le développement rapide des technologies de l'information est aujourd'hui indissociable du fonctionnement quotidien des établissements de santé. Les systèmes d'information hospitaliers constituent le socle numérique permettant de garantir la qualité, la continuité et la sécurité des soins aux patients.

Cependant, cette dépendance croissante expose également les établissements hospitaliers à des menaces majeures. Dans ce contexte, la protection du Système d'Information devient un enjeu stratégique de premier ordre, pour plusieurs raisons essentielles :

- Préserver la qualité des soins en assurant la disponibilité et l'intégrité des outils numériques nécessaires aux actes médicaux et administratifs,
- Protéger les données sensibles (données de santé, données personnelles, informations administratives) contre toute compromission, perte, vol ou destruction,
- Faire face à la montée en puissance des cyberattaques, notamment les attaques par rançongiciels ("ransomware"), les intrusions malveillantes, et les tentatives d'extorsion ciblant spécifiquement les centres hospitaliers,
- Répondre aux exigences légales et réglementaires (RGPD, référentiels de cybersécurité, doctrine de sécurité numérique en santé) imposant une vigilance accrue et des mesures de protection renforcées.

L'actualité démontre que les établissements de santé figurent parmi les cibles privilégiées des cybercriminels, du fait de la valeur inestimable des données médicales et de la sensibilité critique de leurs missions. Une cyberattaque réussie peut entraîner des conséquences dramatiques : interruption des soins, atteinte à la vie des patients, perte de confiance, sanctions juridiques et dommages d'image irréversibles.

Face à cet environnement à risques élevés :

- L’établissement doit garantir une fiabilité sans faille de son Système d’Information,
- La cybersécurité doit être perçue comme une priorité collective à tous les niveaux de l’organisation,
- La sécurité du SI doit faire l'objet d'une démarche d'amélioration continue, intégrant en permanence les innovations technologiques, les meilleures pratiques et les évolutions réglementaires.

La maîtrise de ces enjeux est désormais indispensable pour préserver la confiance des patients, des partenaires et des autorités de tutelle, tout en assurant la pérennité et la résilience des activités hospitalières.

3. Principes fondamentaux de sécurité

La sécurité des systèmes d'information d'un établissement hospitalier repose sur une approche globale et cohérente, combinant les dimensions techniques, organisationnelles et humaines. Elle ne peut être envisagée comme un simple ensemble de mesures isolées, mais comme un écosystème structuré, dont tous les éléments interagissent pour préserver la fiabilité, la disponibilité et la confidentialité des informations critiques.

La démarche de sécurisation s'inscrit dans une gestion dynamique des risques, proportionnée à la criticité des activités de l'établissement. Chaque dispositif, chaque procédure doit être évalué en fonction de son impact potentiel sur la continuité des soins, sur la protection des données sensibles et sur la responsabilité légale de l'établissement.

Dans ce cadre, seuls des produits et services reconnus, éprouvés et, si possible, certifiés, doivent être retenus. Le choix des technologies ne saurait se faire à la légère : il doit reposer sur des critères stricts de robustesse, de conformité aux normes en vigueur et d'aptitude à résister aux menaces évolutives du cyberespace.

La sécurité du système d'information ne peut être figée dans le temps. Elle doit s'inscrire dans une logique d'amélioration continue, en adaptant sans cesse les dispositifs de protection face aux nouvelles vulnérabilités, aux innovations technologiques, et aux enseignements tirés des incidents passés. Ce processus d'évolution permanente est la condition indispensable pour rester à la hauteur des défis contemporains.

Enfin, les politiques et procédures mises en œuvre doivent être accessibles, compréhensibles et applicables par l'ensemble des utilisateurs. Il est impératif que chacun, quel que soit son rôle ou son niveau d'expertise, puisse comprendre les enjeux et adopter les bons comportements. Une sécurité véritablement efficace repose autant sur la performance technique que sur l'adhésion consciente et l'implication active de l'humain.

En complément de l'approche organisationnelle et humaine, la protection du système d'information repose également sur des dispositifs techniques de défense. Le système est notamment protégé par des mécanismes de filtrage réseau et de prévention des intrusions (tels que des pare-feu et des systèmes de détection et de prévention d'intrusions — IDS/IPS), permettant de contrôler rigoureusement les flux entrants et sortants et de détecter toute tentative anormale d'accès ou d'attaque. Ces dispositifs contribuent à la mise en œuvre d'une défense en profondeur, garantissant un haut niveau de sécurité et une réactivité face aux menaces émergentes.

4. Règles de sécurité applicables

4.1 Accès aux actifs informationnels et aux réseaux

- L’accès aux données et aux ressources est strictement limité aux personnes habilitées.
- L'authentification repose sur des méthodes robustes (ex : mots de passe complexes, double authentification).
- Les accès sont attribués selon le principe du "moindre privilège".

4.2 Utilisation d'Internet, de l'intranet et des réseaux

- L'accès à Internet est encadré par des outils de filtrage et de contrôle.
- Les utilisateurs sont responsables de l'usage qu'ils font des outils numériques.
- L'usage à titre personnel est toléré dans les limites du raisonnable et ne doit pas porter atteinte au fonctionnement de l'établissement.

4.3 Utilisation du courrier électronique

- L'email professionnel est réservé aux échanges liés à l'activité professionnelle.
- Les données sensibles doivent être transmises via des moyens de communication sécurisés (chiffrement, plateformes sécurisées).
- Les courriels suspects doivent être immédiatement signalés.

4.4 Télétravail

- L'accès distant aux ressources hospitalières est autorisé via des connexions sécurisées (VPN, chiffrement des échanges).
- Les dispositifs personnels utilisés doivent respecter les standards de sécurité imposés.
- Une authentification forte est obligatoire pour tout accès distant.

4.5 Utilisation des postes fixes et portables

- Les équipements doivent être protégés (mise à jour régulière, verrouillage automatique).
- Les supports de stockage amovibles doivent être restreint.
- Les données professionnelles doivent être conservées uniquement sur les serveurs institutionnels.

4.6 Sauvegarde des données

- Les sauvegardes régulières sont réalisées par l'équipe informatique.
- Les utilisateurs doivent utiliser exclusivement les espaces de stockage sécurisés mis à disposition.

5. Organisation et gouvernance de la sécurité

5.1 Autorités responsables

La gouvernance de la sécurité du système d'information repose sur une implication directe et affirmée de la Direction de l'établissement. Il appartient à la Direction Générale de porter la responsabilité pleine et entière de la définition, de l'adoption et de la mise en œuvre de la Politique de Sécurité du Système d'Information (PSSI). La sécurité du système d'information n'est pas une simple préoccupation technique : elle constitue un enjeu stratégique majeur, engageant l'ensemble des responsabilités de l'établissement, tant sur le plan opérationnel que juridique et éthique.

Pour garantir l'application rigoureuse de cette politique, la Direction procède à la désignation officielle d'un Responsable de la Sécurité du Système d'Information (RSSI). Le RSSI incarne la fonction de référent unique en matière de sécurité numérique. Il est chargé d'assurer la conception opérationnelle, le déploiement, le suivi et l'amélioration continue des mesures de protection. À ce titre, il conseille la Direction, propose les évolutions nécessaires en fonction de l'évolution des menaces, anime la sensibilisation des utilisateurs, pilote les audits de sécurité, supervise la gestion des incidents et produit un reporting régulier sur l'état de la cybersécurité de l'établissement.

La désignation d'un RSSI qualifié et doté des moyens nécessaires n'est pas une option : c'est une condition indispensable pour faire face aux risques croissants et pour garantir la résilience numérique de l'établissement.

5.2 Missions du RSSI

Le Responsable de la Sécurité du Système d'Information (RSSI) occupe une position centrale dans la gouvernance numérique de l'établissement. Il est le pilier stratégique du dispositif de cybersécurité, garant de la résilience et de la confiance numérique au service des missions de soins.

À ce titre, le RSSI a pour mission première de rédiger, de formaliser et de maintenir à jour la Politique de Sécurité du Système d'Information (PSSI), en veillant à ce qu'elle évolue en permanence pour s'adapter aux menaces émergentes, aux évolutions technologiques et aux exigences réglementaires.

Il est également responsable du pilotage des instances de gouvernance de la sécurité : il organise, anime et suit les comités de pilotage, les groupes de travail et les réunions de suivi dédiés à la cybersécurité, assurant ainsi une coordination active entre tous les acteurs concernés.

Le RSSI définit, en concertation avec la Direction et les parties prenantes, les objectifs de sécurité ainsi que les plans d'action annuels visant à renforcer en continu le niveau de protection du système d'information.

Conscient que la sécurité repose aussi sur l'humain, il a pour mission de déployer des campagnes de sensibilisation et de formation, afin de développer une véritable culture de la cybersécurité au sein de l'établissement. Il veille à ce que chaque utilisateur soit acteur de la protection des données.

Le RSSI est également le référent dans la gestion des incidents de sécurité. Il pilote la réponse aux événements, coordonne les mesures correctives et préventives, et établit un rapport annuel détaillé présentant l'état de la sécurité, les incidents recensés, les leçons tirées, ainsi que les axes d'amélioration recommandés.

Enfin, il supervise la réalisation d'audits réguliers et d'opérations de contrôle pour évaluer l'efficacité des dispositifs en place, détecter les vulnérabilités et proposer les adaptations nécessaires.

La mission du RSSI est donc globale, stratégique et opérationnelle, et conditionne directement la capacité de l'établissement à protéger son patrimoine informationnel et à assurer la sécurité de ses missions vitales.

5.3 Comité de Pilotage de la Sécurité du Système d'Information

Un comité de pilotage hebdomadaire assurant la supervision stratégique et la coordination des efforts visant à garantir la sécurité des systèmes d'information, et ainsi préserver l'intégrité, la confidentialité et la disponibilité des données essentielles au bon fonctionnement des missions de soins.

Sous l'autorité de la Direction et en étroite collaboration avec le Responsable de la Sécurité du Système d'Information (RSSI), le COPIL a pour mission de suivre l'exécution des plans d'action sécurité. Il veille à ce que chaque projet, chaque initiative définie dans le cadre de la Politique de Sécurité soit effectivement implémentée, dans le respect des délais, des objectifs et des standards de sécurité. Le COPIL assure également que les ressources nécessaires sont allouées pour mener à bien ces actions.

Étant donné la rapidité avec laquelle évoluent les menaces et les technologies, le COPIL exerce une veille continue sur l'ensemble des risques liés à la sécurité des systèmes d'information. Il adapte les mesures de sécurité en fonction des nouvelles menaces identifiées, des innovations technologiques et des évolutions réglementaires. Cette approche proactive permet à l'établissement de maintenir un niveau de sécurité optimal face à un environnement numérique de plus en plus complexe et vulnérable.

5.4 Rôle des utilisateurs

Les utilisateurs des systèmes d'information de l'établissement jouent un rôle essentiel et fondamental dans la sécurité globale du système d'information. Leur responsabilité va bien au-delà de l'utilisation quotidienne des outils numériques : ils sont les premiers acteurs de la protection des données sensibles, et leur engagement personnel est une condition indispensable pour garantir la sécurité des informations et des infrastructures.

Chaque utilisateur doit accepter et respecter sans réserve la charte d'utilisation des systèmes d'information. Cette charte n'est pas une simple formalité : elle représente l'engagement ferme et conscient de chacun à respecter les règles de sécurité établies pour protéger les données et les systèmes critiques. L'adhésion à cette charte est un acte de responsabilité collective.

De plus, il est impératif que chaque utilisateur suive rigoureusement toutes les consignes de sécurité mises en place. Cela inclut non seulement le respect des procédures liées à l'accès aux données, mais aussi l'application de bonnes pratiques pour éviter toute vulnérabilité (comme l'usage des mots de passe, la gestion des accès, la sécurisation des postes de travail). Ignorer ces consignes peut non seulement entraîner des risques pour la sécurité de l'établissement, mais aussi exposer des données sensibles à des atteintes irréversibles.

Les utilisateurs doivent également agir avec vigilance et réactivité en cas d'incident de sécurité ou de comportement suspect. Il est impératif qu'ils signalent sans délai toute anomalie, tout comportement suspect ou toute tentative d'intrusion, car la rapidité de la réaction est souvent la clé pour limiter les impacts d'une attaque. En n'agissant pas immédiatement, un utilisateur peut être indirectement responsable d'un incident de sécurité majeur.

Enfin, chaque utilisateur endosse la pleine responsabilité de ses actes en matière de sécurité. Cela implique une prise de conscience claire : tout manquement aux règles de sécurité peut entraîner des conséquences graves, non seulement sur le système d’information, mais aussi sur la continuité des soins et sur la protection des données des patients. La sécurité des systèmes d'information est l'affaire de tous, et chaque utilisateur, par ses actions quotidiennes, participe à la construction d'un environnement numérique sécurisé.

6. Plan d'action et évaluation

6.1 Actions de contrôle

Dans un environnement où les menaces évoluent rapidement, il est impératif de mettre en place des mécanismes de contrôle rigoureux et réguliers, afin de détecter et corriger toute vulnérabilité avant qu'elle ne puisse être exploitée.

Ainsi, des contrôles et audits périodiques sont effectués au minimum deux fois par an. Ces audits permettent de vérifier l'application effective des règles de sécurité, en examinant l'ensemble des systèmes, des processus et des pratiques de gestion de la sécurité. Ces évaluations ne se contentent pas d'une simple vérification de la conformité, mais cherchent également à identifier des axes d'amélioration pour rendre le système plus robuste face aux risques croissants.

Ces audits portent une attention particulière aux aspects les plus critiques de la sécurité numérique : l'accès aux données, la gestion des droits utilisateurs, la protection des infrastructures, ainsi que les pratiques en matière de gestion des incidents. Ils permettent de dresser un bilan précis sur l'état de la sécurité des systèmes d'information et d'apporter les ajustements nécessaires en temps réel.

Ainsi afin de renforcer la protection des systèmes d'information et de limiter les risques de propagation d'incidents en cas de compromission, des mesures de segmentation réseau sont mises en œuvre. Les réseaux sont structurés en VLANs distincts correspondant aux différents rôles métiers au sein de l'établissement (administrateurs, médecins, patients, etc.). Cette séparation logique des flux réseau permet de cloisonner les activités, de réduire la surface d'attaque et de contenir tout incident potentiel, évitant ainsi qu'une compromission dans un domaine ne se propage à l'ensemble du système d'information. Cette approche technique s'inscrit dans une démarche globale de défense en profondeur et vient compléter les dispositifs organisationnels et humains déjà mis en place.

6.2 Formation et sensibilisation

La formation et la sensibilisation des utilisateurs aux enjeux de la cybersécurité sont des leviers essentiels pour garantir l'efficacité et la pérennité des mesures de sécurité mises en place. La Direction des Systèmes d'Information (DSI) joue un rôle clé dans cette démarche en proposant des programmes réguliers de sensibilisation et de formation, afin de cultiver une véritable culture de sécurité numérique au sein de l'établissement.

Ces formations sont conçues pour renforcer la vigilance des utilisateurs face aux risques liés aux cyberattaques et pour promouvoir des bonnes pratiques dans l'utilisation des systèmes d'information. Elles couvrent des thématiques variées allant de la gestion des mots de passe à la détection des tentatives de phishing, en passant par l'importance de la protection des données sensibles et des procédures de sécurité à suivre en cas d'incident.

6.3 Sanctions

Le respect des règles définies dans la PSSI est crucial pour maintenir la sécurité des systèmes d'information et protéger les données sensibles de l'établissement. Tout manquement grave aux règles de la PSSI, qu'il s'agisse de négligence, de violation délibérée des consignes de sécurité ou de non-respect des procédures établies, peut avoir des conséquences graves sur la sécurité des systèmes, la confidentialité des données et la continuité des activités de soin. En conséquence, de tels manquements peuvent entraîner des mesures disciplinaires, allant de l'avertissement à des sanctions

plus sévères, voire des mesures judiciaires si la violation des règles constitue une infraction à la législation en vigueur.

6.4 Mise à jour de la politique

La PSSI n'est pas un document figé, mais un outil vivant et évolutif, nécessaire pour répondre aux enjeux croissants de la cybersécurité dans le contexte hospitalier. Ainsi, elle est revue au moins tous les deux ans pour s'assurer qu'elle reste alignée avec les évolutions technologiques, réglementaires et les nouveaux risques identifiés.

Cette révision permet d'ajuster les mesures de sécurité en fonction des changements dans l'architecture des systèmes d'information, de l'émergence de nouvelles menaces ou de modifications législatives et réglementaires. De plus, si des changements significatifs affectent les systèmes d'information (comme l'introduction de nouvelles technologies, l'intégration de nouveaux outils ou l'extension des infrastructures), une mise à jour anticipée de la PSSI peut être nécessaire pour garantir que les mesures de sécurité restent adaptées et efficaces. La mise à jour régulière de la PSSI permet ainsi à l'établissement de maintenir une approche proactive et cohérente face aux défis en constante évolution dans le domaine de la cybersécurité.

7 Mise en application

La présente politique sera mise en application à compter de sa date de validation.