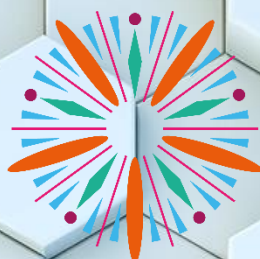


DIRECTION DU SYSTÈME D'INFORMATION ET DU DOSSIER PATIENT
SÉCURITÉ DU SYSTÈME D'INFORMATION



CHU
Poitiers

POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION

DATE DE MISE À JOUR : Août 2022

DIFFUSION PUBLIQUE

SUIVI DU DOCUMENT

VERSION	DATE	NOM	COMMENTAIRE
1.0	2009	ERIC POTAUX	CREATION
1.5	NOVEMBRE 2014	PIERRE TAVEAU	MISE A JOUR SUITE A L'AUDIT DE SECURITE
2.0	MAI 2015	PIERRE TAVEAU	MISE EN CONFORMITE AVEC LA PSSI-E
3.0	SEPTEMBRE 2020	NICOLAS ACQUIER	MISE A JOUR DU DOCUMENT ET DE SA STRUCTURE
4.0	AOUT 2022	NICOLAS ACQUIER	CREATION VERSION PUBLIQUE ET M.àJ VISUELS

Table des matières

1	ENGAGEMENT DE LA DIRECTION GÉNÉRALE	4
2	OBJET DE LA PSSI	5
3	CHAMP D'APPLICATION	5
3.1.1	ENJEUX ET ORIENTATION STRATEGIQUE	5
4	CONTEXTE.....	5
4.1.1	ENJEUX DE SECURITE LIES AU SYSTEME D'INFORMATION.....	5
5	TEXTES ET DOCUMENTS DE RÉFÉRENCE APPLICABLES.....	6
5.1	CADRE LÉGISLATIF ET RÈGLEMENTAIRE.....	6
5.1.1	AU NIVEAU NATIONAL	7
5.1.2	AU NIVEAU EUROPÉEN.....	8
6	NORMES ET DOCUMENTS DE RÉFÉRENCE	8
7	PRINCIPAUX RISQUES LIÉS AU SI	9
7.1	ORIGINE DES RISQUES.....	9
7.2	PRINCIPAUX RISQUES IDENTIFIÉS	9
7.3	STRATEGIE DE TRAITEMENT DES RISQUES	9
8	ORGANISATION DE LA SSI	10
8.1	LES ACTEURS DE LA SSI AU CHU DE POITIERS.....	10
8.2	LES ACTEURS EXTERNES.....	10
8.3	APPLICATION DES MESURES DE SECURITE AU CHU DE POITIERS.....	10
8.4	FORMALISATION DES DOCUMENTS	10
9	RESSOURCES HUMAINES.....	11
9.1	LES UTILISATEURS	11
9.2	LE PERSONNEL PERMANENT	11
9.3	LES MOUVEMENTS DE PERSONNEL.....	11
10	GESTION DES BIENS	12
10.1	CARTOGRAPHIE DES SYSTEMES D'INFORMATION.....	12
10.2	QUALIFICATION ET PROTECTION DES INFORMATIONS.....	12
11	INTÉGRATION DE LA SSI DANS LE CYCLE DE VIE DES SI	12
11.1	GESTION DES RISQUES ET HOMOLOGATION DE SECURITE	12
11.2	MAINTIEN EN CONDITIONS DE SECURITE	13
11.3	PRODUITS ET SERVICES LABELISES	13
11.4	GESTION DES PRESTATAIRES	13
12	SÉCURITÉ	14
12.1	SÉCURITÉ PHYSIQUE	14
12.2	SÉCURITÉ DES RÉSEAUX	15
12.3	SÉCURITÉ DU POSTE DE TRAVAIL	17
12.4	SÉCURITÉ DU DEVELOPPEMENT DES SYSTÈMES	20
13	ARCHITECTURE DES SI	21

13.1	ARCHITECTURE SECURISEE DES CENTRES INFORMATIQUES	21
14	EXPLOITATION DES SI.....	21
14.1	PROTECTION DES INFORMATIONS SENSIBLES.....	21
14.2	SURVEILLANCE ET CONFIGURATION DES RESSOURCES INFORMATIQUES.....	22
14.3	GESTION DES AUTORISATIONS ET CONTROLES D'ACCES LOGIQUE AUX RESSOURCES	22
14.4	PROCESSUS D'AUTORISATION	22
14.5	GESTION DES IDENTIFIANTS.....	23
14.6	GESTION DES AUTHENTIFICATIONS D'ADMINISTRATION.....	23
14.7	ADMINISTRATION DES SYSTEMES.....	24
14.8	ADMINISTRATION DES DOMAINES	24
14.9	ENVOI EN MAINTENANCE ET MISE AU REBUT.....	25
14.10	LUTTE CONTRE LES CODES MALVEILLANTS	25
14.11	MISE A JOUR DES SYSTEMES ET DES LOGICIELS	26
14.12	JOURNALISATION.....	26
14.13	GESTION DYNAMIQUE DE LA SECURITE	27
14.14	GESTION DES MATERIELS INFORMATIQUES FOURNIS A L'UTILISATEUR	27
14.15	NOMADISME.....	27
14.16	SECURITE DES RESSOURCES INFORMATIQUES.....	28
15	TRAITEMENT DES INCIDENTS	29
15.1	CHAINES OPERATIONNELLES.....	29
15.2	TRAITEMENT DES ALERTES DE SECURITE EMISES PAR LES INSTANCES NATIONALES	29
15.3	REMONTEE DES INCIDENTS DE SECURITE RENCONTRES	29
16	REPRISE D'ACTIVITÉ	30
16.1	DEFINITION DU PRA DES SI	30
16.2	MISE EN ŒUVRE DU PRA DES SI.....	30
16.3	MAINTIEN EN CONDITIONS OPERATIONNELLES DU PRA DES SI.....	30
17	CONFORMITÉ, AUDIT, INSPECTION, CONTRÔLE	31
17.1	CONTROLES REGULIERS.....	31
18	PLAN D'ACTIONS.....	31
19	OPERATEUR DE SERVICES ESSENTIELS.....	31
19.1	SYSTÈMES D'INFORMATION ESSENTIELS	31
19.2	HOMOLOGATION DES SYSTÈMES D'INFORMATION ESSENTIELS	31
20	GLOSSAIRE ET LISTE DES ABRÉVIATIONS	32
21	ANNEXES.....	33
	ANNEXE 1 : FONCTION SÉCURITÉ	33
	ANNEXE 2 : MÉTRIQUES D'ANALYSE DE RISQUES	34
	ÉCHELLE DE NIVEAUX DE GRAVITÉ	34
	ÉCHELLE DE NIVEAUX DE VRAISEMBLANCE.....	35
	ÉCHELLE DE NIVEAU DE RISQUE	36
	ANNEXE 3 : DOCUMENTS DE RÉFÉRENCE.....	37

1 ENGAGEMENT DE LA DIRECTION GÉNÉRALE

Les patients, leurs proches, les professionnels du CHU, mais aussi les étudiants et les élèves de nos écoles et instituts nous font confiance.

Bien entendu, ils attendent de nous des soins de qualité et un enseignement susceptible de les doter de solides connaissances et compétences.

L'utilisation massive des technologies de l'information doit faire face à une augmentation croissante des risques accidentels ou d'origines malveillantes, il est donc fondamental de protéger nos informations ainsi que celles qui nous sont confiées.

Chacun doit être conscient qu'un manque de protection de notre système d'information peut entraîner de véritables dommages sur nos valeurs, notamment :

- Φ La sécurité des patients ;
- Φ La confiance des usagers ;
- Φ Le respect des obligations légales ;
- Φ La protection de la vie privée et la sécurité des données médicales et personnelles.

Pour ce faire, nous mobilisons des ressources techniques et informatiques, des réseaux, des infrastructures et des équipements qui doivent fournir l'information, la traiter, la stocker mais qui doivent aussi en garantir l'absolue sécurité, ce qui signifie son intégrité et sa disponibilité.

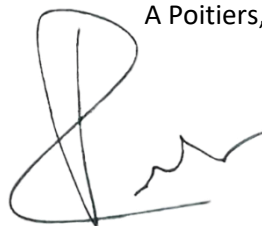
C'est pourquoi, conformément au cadre légal et réglementaire, nous avons désigné un responsable de la sécurité du système d'information, dénommé ci-après « RSSI », chargé de définir et de coordonner la mise en application d'une politique de sécurité du système d'information, en conformité avec les exigences réglementaires et normatives, afin de répondre aux missions spécifiques de nos directions métiers et à la satisfaction des besoins des usagers.

La présente politique de sécurité du système d'information constitue le cadre unique de référence du CHU de Poitiers pour toutes les questions de sécurité du système d'information.

Chacun doit être conscient que le respect des règles formalisées dans les règlements, chartes et politiques de sécurité est un élément essentiel pour la protection de notre système d'information. Chaque responsable de service doit communiquer cette politique et s'assurer que les règles sont respectées au sein de son service.

Enfin, nous nous engageons à mettre à disposition les moyens nécessaires pour permettre le bon maintien en conditions de sécurité du système d'information du CHU de Poitiers.

A Poitiers, le 9 Octobre 2020



Anne Costa
Directrice Générale

2 OBJET DE LA PSSI

La Politique de Sécurité du Système d'Information (ci-après « la PSSI ») du CHU de Poitiers est un document de référence, validé et appuyé par la direction, qui doit être pris en compte par l'ensemble des acteurs et utilisateurs du système d'information. Il décrit les principaux enjeux de la sécurisation du SI du CHU de Poitiers ainsi que les normes et exigences permettant un maintien en conditions de sécurité.

Les différentes mesures qu'elle prévoit sont destinées à être mises en œuvre de manière graduelle, définie par un Plan d'Action Sécurité, afin de permettre une progression de la sécurité du système d'information acceptable par la structure et d'atteindre le niveau de sécurité requis.

3 CHAMP D'APPLICATION

Le champ d'application de la PSSI concerne l'architecture matérielle et logicielle du système d'information du CHU de Poitiers.

3.1.1 ENJEUX ET ORIENTATION STRATEGIQUE

La PSSI représente les bonnes pratiques à mettre en œuvre pour assurer les 4 axes de la sécurité des informations traitées au CHU de Poitiers :

- Φ La disponibilité ;
- Φ L'intégrité ;
- Φ La confidentialité ;
- Φ La traçabilité.

Tout cela en prenant en compte le contexte réglementaire auquel le CHU de Poitiers est soumis.

4 CONTEXTE

4.1.1 ENJEUX DE SECURITE LIES AU SYSTEME D'INFORMATION

L'informatisation du dossier patient, et de l'ensemble des processus de production de soins (prescription, dispensation, administration), permet d'améliorer la sécurité et la qualité des soins au sein du CHU de POITIERS. Elle exige que le système d'information puisse fonctionner en continu (haute disponibilité : 24h/24, 7j/7), conserver les données dans le temps tout en préservant leur intégrité, et garantir la confidentialité des informations médicales dans des environnements ouverts et partagés.

Dans le même temps, les systèmes d'informations du CHU de Poitiers deviennent de plus en plus :

- Φ Connectés : ils intègrent la gestion des équipements biomédicaux et l'exploitation des informations qu'ils produisent, les demandes d'accès au système d'information se diversifient avec l'usage de terminaux « mobiles » (smartphones, tablettes, ordinateurs portables) ...
- Φ Ouverts : pour favoriser la coordination des soins avec les autres acteurs de santé et permettre de mieux prendre en charge le patient tout au long de son parcours de soins : échange d'information médicale par messagerie sécurisée, partage de documents médicaux avec le DMP (Dossier Médical Personnel), coopération dans le cadre de réseaux de santé, développement de la télémedecine ...
- Φ Mutualisés dans le cadre du Groupement Hospitalier de Territoire (GHT 86).

Le système d'information s'appuie sur un ensemble de plus en plus grand de dispositifs, interconnectés ou cohabitant, au service des professionnels de santé et pour le bénéfice d'une meilleure prise en charge du patient et d'amélioration du système de santé.

Levier d'amélioration de la qualité des soins et d'efficience, il s'accompagne d'un accroissement significatif des vulnérabilités, des menaces et des risques d'atteinte aux informations conservées sous forme électronique et en conséquence aux processus de soins s'appuyant sur les systèmes d'information de santé. L'origine de ces menaces peut être intentionnelle (développement de la cybercriminalité, acte de malveillance d'un utilisateur du système d'information), ou involontaire (faille technique, manque de sensibilisation des utilisateurs...).

Dès lors, la sécurité de nos systèmes d'information est une condition indispensable pour garantir une bonne prise en charge des patients et une gestion intègre du CHU de Poitiers.

La maîtrise de la sécurité des systèmes d'information doit être intégrée tout au long du cycle de vie de ces systèmes. Elle doit s'appliquer aux dispositifs et applications en place, et accompagner l'intégration des nouvelles applications.

Elle doit prendre en compte l'évolution des facteurs, tant internes qu'externes, qui sont susceptibles de l'impacter : usage au quotidien des informations dématérialisées, stockage d'informations médicales à caractère personnel rendu facilement accessibles, responsabilité de l'organisme quant au respect du décret confidentialité.

Elle doit en outre garantir la disponibilité des services du système d'information et offrir un socle de données fiables, intègres, et dont la confidentialité est protégée chaque fois que nécessaire.

La sécurité informatique doit s'inscrire dans une démarche « qualité » et de maîtrise global des risques, en recherchant l'adhésion des utilisateurs. Il est important de conserver à l'esprit que la capacité de protection et de réaction repose bien souvent in fine sur l'utilisateur.

5 TEXTES ET DOCUMENTS DE RÉFÉRENCE APPLICABLES

5.1 CADRE LÉGISLATIF ET RÉGLEMENTAIRE

La PSSI est encadrée par un ensemble de textes réglementaires précisant les possibilités de mise en œuvre ainsi que les droits et devoirs tant des équipes techniques que des utilisateurs.

La plupart des textes qui s'appliquent au SI de l'établissement sont codifiés dans les codes suivants :

- Φ Code de la Santé Publique ;
- Φ Code de l'Action Sociale et des Familles ;
- Φ Code des Postes et Télécommunications ;
- Φ Code du Patrimoine ;
- Φ Code Civil ;
- Φ Code Pénal.

La législation est Nationale et Européenne.

5.1.1 AU NIVEAU NATIONAL

- Φ **La loi du 6 Janvier 1978** relative à l'informatique, aux fichiers et aux libertés, modifiée en 2004. (Voir loi du 29 décembre 1990, loi du 1^{er} Juillet 1992, loi du 22 Juillet 1992, loi du 26 Juillet 1996) ;
- Φ **La loi du 12 juillet 1980** relative à la preuve des actes juridiques ;
- Φ **L'arrêté du 28 octobre 1980** qui définit un certain nombre de termes français de l'informatique et qui impose aux administrations, en particulier à l'Education Nationale, de les employer ;
- Φ **Les lois Auroux du 28 octobre 1982** qui comportent des dispositions relatives à l'introduction de nouvelles technologies dans l'entreprise :
 - Lors d'une automatisation, la direction d'une entreprise doit faire part de ses projets et consulter le comité d'entreprise (qui n'a pas cependant le droit de veto) ;
 - Elle doit mettre à la disposition du C.E. tous moyens d'évaluer le projet du point de vue des conditions de travail, y compris le financement éventuel de l'intervention d'un conseil extérieur désigné par le C.E.
- Φ **Le décret du 15 novembre 1985** portant publication de la Convention pour la protection des personnes à l'égard du traitement automatique de données à caractère personnel ;
- Φ **La loi du 29 décembre 1990**, modifiée par la loi du 11 juillet 1991, notamment son article 28 réglementant la cryptologie ;
- Φ **Le décret du 14 mai 1991** relatif à la prévention des risques liés au travail sur des équipements comportant des écrans de visualisation. Ce décret comporte peu d'obligations précises et ne prévoit pas de sanctions, mais il émet un certain nombre de principes, parmi lesquels :
 - L'employeur est tenu de procéder à une analyse des risques professionnels et des conditions de travail pour tous les postes comportant un écran de visualisation.
 - L'employeur est tenu d'organiser le travail de telle sorte que l'activité du travailleur soit interrompue par des pauses adaptées au type de travail.
 - Le logiciel doit être d'un usage facile, adapté à la tâche et au niveau de connaissances et d'expérience de l'utilisateur.
 - Un travailleur ne peut être affecté à des travaux de visualisation que s'il a fait l'objet d'un examen médical des yeux et, si nécessaire, les dispositifs de corrections normaux doivent être utilisés.
 - Le matériel doit satisfaire à un ensemble de critères ergonomiques.
- Φ **La loi du 20 juin 1992** qui soumet à l'obligation du dépôt légal les progiciels, bases de données, systèmes experts et autres produits de l'intelligence artificielle dès lors que ces produits sont mis à disposition du public par la diffusion d'un support matériel ;
En sont donc exclus les produits auxquels on accède en ligne.
- Φ **La loi du 1er juillet 1992** relative au code de la propriété intellectuelle (remplaçant celles du 11/03/1957 et du 3/07/1985). Les droits des auteurs de logiciels sont protégés par cette loi.
 - Ce code de la propriété intellectuelle rassemble, met à jour et synthétise tous les textes traitant de la propriété des œuvres littéraires et artistiques, des logiciels, des œuvres audio-visuelles et des inventions.
- Φ **La loi du 22 juillet 1992** (nouveau Code Pénal) relative aux délits informatiques définissant comme infractions les actions suivantes à l'égard de tout système de traitement automatisé de données :
 - Y accéder ou s'y maintenir frauduleusement ;

- Entraver ou fausser son fonctionnement ;
- Y introduire, supprimer ou modifier frauduleusement des données.
- Φ **La loi du 21 janvier 1995** d'orientation et de programmation relative à la sécurité (voir aussi le décret du 17 octobre 1996).
 - L'article 10 de cette loi régit les opérations de vidéo surveillance sur la voie publique et les lieux ouverts au public.
- Φ **La loi du 26 juillet 1996** réglementant les télécommunications.
- Φ **L'article 17 modifie l'article 28 de la loi du 29 décembre 1990 sur les prestations de cryptologie.**
- Φ **Le décret du 17 octobre 1996** relatif à la vidéo surveillance pour application de la loi du 21 janvier 1995.
- Φ **Décret no 98-101 du 24 février 1998** définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie ;
- Φ **Décret no 98-102 du 24 février 1998** définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications ;
- Φ **Décret no 98-206 du 23 mars 1998** définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.
- Φ **Décret no 98-207 du 23 mars 1998** définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.

5.1.2 AU NIVEAU EUROPÉEN

- Φ **La loi du 10 Mai 1994** portant mise en œuvre de la directive européenne du 14 Mai 1991 et modifiant le Code de la Propriété Individuelle ;
- Φ **La directive européenne du 24 octobre 1995** concernant toutes les données à caractère personnel relatives à une personne identifiée ou identifiable ;
- Φ **La directive européenne du 11 mars 1996** relative à la protection des Bases de Données.

6 NORMES ET DOCUMENTS DE RÉFÉRENCE

Les textes mentionnés ci-après s'imposent aux structures qui relèvent du secteur public et doivent être pris en compte pour l'élaboration et la mise en œuvre de la PSSI :

- Φ Référentiel Général de Sécurité (RGS) ;
- Φ Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) ;
- Φ Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) ;
- Φ Politique Ministérielle de Sécurité des Systèmes d'Information (PMSSI) ;
- Φ Politique de Sécurité des Systèmes d'Information du Ministère Chargé des Affaires Sociales (PSSI MCAS) ;
- Φ Directive NIS (Network & Information Security) ;
- Φ Instruction N°SG/DSSIS/2016/309 Plan d'action SSI ;
- Φ Hôpital Numérique Ouvert sur son Environnement (HOP'EN) ;
- Φ La certification des comptes, notamment la partie audit du système d'information.

Les textes mentionnés ci-après ne sont pas de nature impérative, mais sont utiles comme références pour l'élaboration ou la mise en œuvre de la PSSI :

- Φ Recommandations techniques de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

7 PRINCIPAUX RISQUES LIÉS AU SI

7.1 ORIGINE DES RISQUES

La PSSI considère les risques dont l'origine peut être :

- Φ Une catastrophe naturelle ou un accident industriel d'ampleur locale ;
- Φ Une défaillance technique ;
- Φ Une erreur ou un acte de malveillance commis par :
 - Le personnel interne ;
 - Les sous-traitants et les fournisseurs ;
 - Les usagers et les visiteurs ;
 - Les délinquants ou criminels potentiellement auteur de vols ou de vandalisme ;
 - Les « cybercriminels » ne visant pas spécifiquement la structure.

La PSSI ne prend pas en compte certaines menaces d'origine particulière, les scénarios associés étant très peu vraisemblables dans le contexte de la structure et impliquant des coûts de protection incompatibles avec son activité. Ces origines non prises en compte sont :

- Φ Les menaces d'origine étatique (quel qu'il soit) ;
- Φ Les « cybercriminels » qui viseraient spécifiquement la structure et disposeraient des moyens nécessaires ;

La PSSI ne considère pas non plus les atteintes de type « espionnage industriel », la structure ne pratiquant pas d'activité de recherche dans des secteurs jugés fortement concurrentiels.

7.2 PRINCIPAUX RISQUES IDENTIFIÉS

Le niveau de risque associé à chaque risque (scénario combinant un événement redouté avec un ou plusieurs scénarios de menace) découle de la gravité de l'évènement redouté (gravité de ses impacts) et de la vraisemblance des scénarios de menace. Le niveau de risque indiqué correspond au risque « brut », c'est-à-dire en présence de l'ensemble des vulnérabilités potentielles et avant qu'aucune mesure de sécurité du SI ne soit mise en œuvre.

Les métriques utilisées pour qualifier les niveaux de gravité et de vraisemblance et la règle de combinaison de ces deux échelles pour en déduire le niveau de risque sont détaillées en Annexe 2.

Les risques identifiés pour le SI du CHU de Poitiers ne sont pas décrits dans cette version publique de la PSSI.

7.3 STRATEGIE DE TRAITEMENT DES RISQUES

Les mesures de SSI mises en œuvre doivent viser à réduire l'ensemble des risques liés au SI.

Avec l'application de ces mesures, le risque résiduel doit être ramené à un niveau de risque « limité », que ce soit par la réduction des cas de réalisation des scénarios redoutés ou par la limitation de leur impact en termes d'effet et de durée.

Le poids de ce risque résiduel peut être en partie partagé avec des organismes d'assurance.

Cette stratégie de réduction des risques s'appuie sur des mesures organisationnelles continues et des moyens techniques ad hoc dans l'ensemble du SI.

L'ensemble des mesures identifiées sont détaillées dans le plan d'actions de mise en œuvre de la PSSI.

8 ORGANISATION DE LA SSI

Les exigences relatives à l'organisation de la sécurité du système d'information sont décrites ci-après :

8.1 Les acteurs de la SSI au CHU de Poitiers

8.1.1 – ORG-RSSI : Désignation du responsable SSI

L'Autorité Qualifiée en Sécurité des Systèmes d'Information (AQSSI) s'appuie sur un Responsable de la Sécurité du Système d'Information (RSSI), chargé de l'assister dans le pilotage et la gestion de la SSI. Le RSSI fait valider les mesures d'application de la PSSI par l'autorité qualifiée et veille à leur application.

8.1.2 – ORG-RESP : Formalisation des responsabilités

Une note d'organisation fixe la répartition des responsabilités et rôles en matière de SSI. Cette note précise la constitution et le rôle du comité de sécurité.

8.2 Les acteurs externes

8.2.1 – ORG-TIERS : Gestion contractuelle des tiers

Le RSSI coordonne les actions permettant l'intégration des clauses liées à la SSI dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques.

8.3 Application des mesures de sécurité au CHU de Poitiers

8.3.1 – ORG-APP-INSTR : Application de l'instruction au CHU

Le RSSI planifie les actions de mise en application de la PSSI. Il rend compte régulièrement de la mise en application des mesures de sécurité auprès de son autorité qualifiée ; et sur demande au FSSI du ministère de tutelle.

8.4 Formalisation des documents

8.4.1 – ORG-APP-DOCS : Formalisation de documents d'application

Le RSSI formalise et tient à jour les documents d'application, approuvés par l'autorité qualifiée, permettant la mise en œuvre des mesures de la PSSI.

9 RESSOURCES HUMAINES

Les exigences relatives aux ressources humaines en termes de sécurité du système d'information sont décrites ci-après :

9.1 Les utilisateurs

9.1.1 – RH-SSI : Charte d'application SSI

Une charte d'utilisation des ressources informatiques, récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques et élaborée sous le pilotage de la chaîne fonctionnelle SSI, est communiquée à l'ensemble des agents du CHU. Cette charte est opposable juridiquement et intégrée au règlement intérieur de CHU. Le personnel non permanent (stagiaires, intérimaires, prestataires...) est informé de ses devoirs dans le cadre de son usage des SI du CHU.

9.2 Le personnel permanent

9.2.1 – RH-MOTIV : Choix et sensibilisation des personnes tenant des postes clés de la SSI

Une attention particulière doit être portée au recrutement des personnes-clés de la SSI : RSSI, correspondants SSI locaux et administrateurs de sécurité. Le RSSI et leurs correspondants SSI locaux doivent être spécifiquement formés à la SSI. Les administrateurs des SI doivent être régulièrement sensibilisés aux devoirs liés à leur fonction, et doivent veiller à respecter ces exigences dans le cadre de leurs activités quotidiennes.

9.2.2 – RH-CONF : Personnels de confiance

Toutes les personnes manipulant des informations sensibles doivent le faire avec une attention et une probité particulière, dans le respect des textes en vigueur. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont rappelées.

9.2.3 – RH-UTIL : Sensibilisation des utilisateurs des systèmes d'information

Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant, et motivé à leur respect.

Il doit être formé à l'utilisation des outils de travail conformément aux règles SSI.

9.3 Les mouvements de personnel

9.3.1 – RH-MOUV : Gestion des arrivées, des mutations et des départs

Une procédure permettant de gérer les arrivées, les mutations et les départs des collaborateurs dans les SI doit être formalisée, et appliquée strictement. Cette procédure doit couvrir au minimum :

- Φ La gestion/révocation des comptes et des droits d'accès aux SI, y compris pour les partenaires et les prestataires externes ;
- Φ La gestion du contrôle d'accès aux locaux ;
- Φ La gestion des équipements mobiles ;
- Φ La gestion du contrôle des habilitations.

10 GESTION DES BIENS

Les exigences relatives à la gestion des biens en termes de sécurité du système d'information sont décrites ci-après :

10.1 Cartographie des systèmes d'information

10.1.1 – GDB-INVENT : Inventaire des ressources informatiques

La DSI établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire est tenu à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle. Il comprend la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes. Il est constitué d'une base de données de configuration, maintenue à jour et tenue à disposition du RSSI.

L'historique des attributions des biens inventoriés doit être conservé, dans le respect de la législation.

10.1.2 – GDB-CARTO : Cartographie

La cartographie précise les centres informatiques, les architectures des réseaux (sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées) et qualifie le niveau de sécurité attendu. Cette cartographie est maintenue à jour et tenue à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle.

10.2 Qualification et protection des informations

10.2.1 – GDB-QUALIF-SENSI : Qualification des informations

La sensibilité de toute information doit être évaluée. Le marquage systématique des documents, en fonction du niveau de sensibilité, est fortement recommandé.

10.2.2 – GDB-PROT-IS : Protection des informations

L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction.

11 INTÉGRATION DE LA SSI DANS LE CYCLE DE VIE DES SI

Les exigences relatives à l'intégration de la sécurité du système d'information dans le cycle de vie du système d'information sont décrites ci-après :

11.1 Gestion des risques et homologation de sécurité

11.1.1 – INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d'information

Tout système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise par l'autorité d'homologation (désignée par l'autorité qualifiée), le cas échéant après avis de la commission d'homologation. Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi.

11.2 Maintien en conditions de sécurité

11.2.1 – INT-SSI : Intégration de la sécurité dans les projets

La sécurité des systèmes d'information doit être prise en compte dans toutes les phases des projets informatiques, sous le contrôle de l'autorité d'homologation, de la conception et de la spécification du système jusqu'à son retrait du service. Une fiche sécurité est incluse dans la méthode de gestion des projets, mise en place à la DSI.

11.2.2 – INT-QUOT-SSI : Mise en œuvre au quotidien de la SSI

La sécurité des systèmes d'information se traite au quotidien par des pratiques d'hygiène informatique. Des procédures écrites définissent les actes élémentaires du maintien en condition de sécurité lors des phases de conception, évolution ou retrait d'un système.

11.2.3 – INT-TDB : Créer un tableau de bord SSI

Un tableau de bord SSI est mis en place et tenu à jour. Il fournit au RSSI et à l'autorité qualifiée (AQSSI), une vision générale du niveau de sécurité et de son évolution, rendant ainsi plus efficace le pilotage de la SSI. Au niveau stratégique, le tableau de bord SSI permet de suivre l'application de la politique de sécurité et de disposer d'éléments propres à qualifier les ressources devant être allouées à la SSI. Au niveau du pilotage, la mise en place de ce tableau de bord permet de contrôler la réalisation d'objectifs opérationnels, d'améliorer la qualité de service et de détecter au plus tôt les retards dans la réalisation de certains objectifs de sécurité.

11.3 Produits et services labélisés

11.3.1 – INT-AQ-PSL : Acquisition de produits et services de confiance

Lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI doivent être utilisés.

11.4 Gestion des prestataires

11.4.1 – INT-PRES-CS : Clauses de sécurité

Toute prestation dans le domaine des SI est encadrée par des clauses de sécurité. Ces clauses spécifient les mesures SSI que le prestataire doit respecter dans le cadre de ses activités.

11.4.1 – INT-PRES-CNTRL : Suivi et contrôle des prestations fournisseurs

Le maintien d'un niveau de sécurité au cours du temps nécessite un contrôle, effectué périodiquement par l'équipe encadrant la prestation, qui porte sur les actions du sous-traitant et la conformité au cahier des charges ;

11.4.1 – INT-REX-AR : Analyse des risques

Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

11.4.1 – INT-REX-HB : Hébergement

L'hébergement des données sensibles de l'administration sur le territoire national est obligatoire, sauf accord du HFDS, et dérogation dûment motivée et précisée dans la décision d'homologation.

11.4.1 – INT-REX-HS : Hébergement et clauses de sécurité

Tout contrat d'hébergement détaille les dispositions mises en œuvre pour prendre en compte la SSI. Ce sont notamment les mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes, etc.).

12 SÉCURITÉ

12.1 SÉCURITÉ PHYSIQUE

Les exigences relatives à la sécurité physique du système d'information sont décrites ci-après :

12.1.1 – PHY-ZONES : Découpage des sites en zones de sécurité

Un découpage des sites en zones physiques de sécurité doit être effectué, en liaison avec le RSSI, les correspondants locaux SSI et les services en charge : de l'immobilier, de la sécurité et des moyens généraux. Pour chaque zone de sécurité, des critères précis d'autorisation d'accès sont établis.

Règles de sécurité s'appliquant aux zones accueillant du public

12.1.2 – PHY-PUBL : Accès réseau en zone d'accueil au public

Tout accès réseau installé dans une zone d'accueil du public doit être filtré ou isolé du reste du réseau informatique du CHU.

Règles de sécurité s'appliquant aux locaux techniques

12.1.3 – PHY-TECH : Sécurité physique des locaux techniques

L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, ou des équipements de réseau et de téléphonie, doit être physiquement protégé.

12.1.4 – PHY-TELECOM : Protection des câbles électriques et de communication

L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, ou des équipements de réseau et de téléphonie, doit être physiquement protégé.

12.1.5 – PHY-CTRL : Contrôles anti-piégeages

Sur les SI particulièrement sensibles, il convient de mener des contrôles anti-piégeages réguliers, effectués par du personnel formé. Il peut être fait appel à des services spécialisés.

12.1.6 – PHY-CI-HEBERG : Convention de service en cas d'hébergement tiers

Dans le cas où un tiers gère tout ou partie des locaux du centre informatique, une convention de service, définissant les responsabilités mutuelles en matière de sécurité, doit être établie entre ce tiers et le CHU.

Règles de sécurité complémentaires s'appliquant aux zones internes et restreintes

12.1.7 – PHY-CI-CTRLACC : Contrôle d'accès physique

L'accès aux zones internes (autorisées uniquement au personnel du centre informatique ou aux visiteurs accompagnés) et restreintes (autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) doit reposer sur un dispositif de contrôle d'accès physique. Ce dispositif doit s'appuyer sur des produits qualifiés, lorsqu'ils sont disponibles, et bénéficier d'un maintien en condition de sécurité rigoureux.

12.1.8 – PHY-CI-MOYENS : Délivrance des moyens d'accès physique

La délivrance des moyens d'accès physique doit respecter un processus formel permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles (entretien ou réparation des bâtiments, des équipements non informatiques, nettoyage, visiteurs, ...), intervient systématiquement et impérativement sous surveillance permanente.

12.1.9 – PHY-CI-TRACE : traçabilité des accès

Une traçabilité des accès, par les visiteurs externes, aux zones restreintes doit être mise en place. Ces traces sont alors conservées un an, dans le respect des textes protégeant les données personnelles.

Règles de sécurité complémentaires s'appliquant aux salles informatiques et locaux techniques**12.1.10 – PHY-CI-ENERGIE : Local énergie**

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

12.1.11 – PHY-CI-CLIM : Climatisation

Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique doit être installé. Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement. Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

12.1.12 – PHY-CI-INC : Lutte contre l'incendie

L'installation de matériel de protection contre le feu est obligatoire. Des procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu ne doit être entreposé dans ces locaux.

12.1.13 – PHY-CI-EAU : Lutte contre les voies d'eau

Une étude sur les risques dus aux voies d'eau doit être réalisée. Cette étude doit notamment prendre en compte le risque de fuite sur un collecteur d'eau douce.

Système d'information de sûreté**12.1.14 – PHY-SI-SUR : Sécurisation du SI de sûreté**

Pour les sites physiques considérés comme importants, des mesures de protection doivent être définies et appliquées en se basant sur les conclusions d'une analyse de risques. L'analyse de risques conduit à la désignation des briques essentielles dont il faut assurer la protection contre des actes malveillants. Un système de gestion de la sécurité du SI de sûreté assure le maintien en condition de sécurité. L'emploi de produits labellisés, quand ils existent, est fortement recommandé.

12.2 SÉCURITÉ DES RÉSEAUX

Les exigences relatives à la sécurité des réseaux du système d'information sont décrites ci-après :

Usage sécurisé des réseaux nationaux**12.2.1 – RES-MAITRISE : Systèmes autorisés sur le réseau**

Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local du CHU.

12.2.2 – RES-INTERCO : Interconnexion avec des réseaux externes

Toute interconnexion entre les réseaux locaux du CHU et un réseau externe (réseau d'un tiers, Internet, etc.) est réalisée soit via le réseau RENATER avec l'utilisation d'un canal sécurisé soit via une ligne spécialisée sécurisée.

12.2.3 – RES-ENTSOR : Mettre en place un filtrage réseau pour les flux entrants et sortants

Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur sont filtrées.

Usage sécurisé des réseaux locaux**12.2.4 – RES-CLOIS : Cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes**

Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.

12.2.5 – RES-RESS : Cloisonnement des ressources en cas de partage de locaux

Dans le cas où le CHU partage des locaux (bureaux ou locaux techniques) avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Si le cloisonnement n'est pas physique, les mesures prises doivent être validées par le ou les RSSI concernés.

Accès spécifiques**12.2.6 – RES-INTERNET-SPECIFIQUE : Cas particulier des accès spécifiques**

Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage métier ne peuvent être mis en place que sur dérogation dûment justifiée, et sur des machines isolées physiquement et séparées du réseau du CHU, après validation préalable de l'autorité d'homologation, ou par délégation du RSSI.

Usage sécurisé des réseaux sans-fil**12.2.7 – RES-SSFIL : Mise en place de réseaux sans-fil**

Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, validées par le RSSI, doivent être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio. À défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des SI manipulant des données sensibles est à proscrire.

Sécurisation des mécanismes de commutation et de routage**12.2.8 – RES-COUCHBAS : Planter des mécanismes de protection contre les attaques sur les couches basses**

Une attention particulière doit être apportée à l'implantation des protocoles de couches basses, de façon à se prémunir des attaques usuelles par saturation ou empoisonnement de cache. Cela concerne, par exemple, le protocole ARP.

12.2.9 – RES-ROUTDYN : Surveiller les annonces de routage

Lorsque l'utilisation de protocoles de routage dynamiques est nécessaire, celle-ci doit s'accompagner de la mise en place d'une surveillance des annonces de routage, et de procédures permettant de réagir rapidement en cas d'incidents.

12.2.10 – RES-SECRET : Modifier systématiquement les éléments d'authentification par défaut des équipements et services

Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.

12.2.11 – RES-DURCI : Durcir les configurations des équipements de réseaux

Les équipements de réseaux (comme les routeurs) doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et certificats, la désactivation des interfaces et services inutiles, ainsi que la mise en place de mécanismes de protection du plan de contrôle.

Cartographie réseau**12.2.12 – RES-CARTO : Elaborer les documents d'architecture technique et fonctionnelle**

L'architecture réseau du système d'information doit être décrite et formalisée à travers des schémas d'architecture, et des configurations, maintenus au fil des évolutions apportées au SI. Les documents d'architecture sont sensibles et font l'objet d'une protection adaptée. La cartographie réseau s'insère dans la cartographie globale des SI.

12.3 SÉCURITÉ DU POSTE DE TRAVAIL

Les exigences relatives à la sécurité des postes de travail du système d'information sont décrites ci-après :

Mise à disposition du poste**12.3.1 – PDT-GEST : Fourniture et gestion des postes de travail**

Les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par l'équipe du domaine Infrastructure chargée des SI.

12.3.2 – PDT-CONFIG : Formalisation de la configuration des postes de travail

Une procédure formalisée de configuration des postes de travail est établie

Sécurité physique des postes de travail**12.3.3 – PDT-VERROUIL-FIXE : Verrouillage de l'unité centrale des postes fixes**

Lorsque l'unité centrale d'un poste fixe est peu volumineuse, donc susceptible d'être facilement emportée, elle doit être protégée contre le vol par un système d'attache (par exemple un câble antivol).

12.3.4 – PDT-VERROUIL-PORT : Verrouillage des postes portables

Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation.

Réaffectation du poste et récupération d'informations**12.3.5 – PDT-REAFFECT : Réaffectation du poste de travail**

Une procédure SSI définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.

Gestion des privilèges sur les postes de travail

12.3.6 – PDT-PRIVIL : Privilèges des utilisateurs sur les postes de travail

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

12.3.7 – PDT-PRIV : Utilisation des privilèges d'accès « administrateurs »

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

12.3.8 – PDT-ADM-LOCAL : Gestion du compte « administrateur local »

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

Protection des informations

12.3.9 – PDT-STOCK : Stockage des informations

Dans la mesure du possible, les données traitées par les utilisateurs sont stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences du CHU et en accord avec les règles de sécurité en vigueur.

12.3.10 – PDT-SAUV-LOC : Sauvegarde / Synchronisation des données locales

Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs.

12.3.11 – PDT-PART-FIC : Partage des fichiers

Le partage de répertoires ou de données hébergées localement sur les postes de travail n'est pas autorisé.

12.3.12 – PDT-SUPPR-PART : Suppression des données sur les postes partagés

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

12.3.13 – PDT-CHIFF-SENS : Chiffrement des données sensibles

Une solution de chiffrement labellisée doit être mise à disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

Nomadisme

12.3.14 – PDT-NOMAD-ACCESS : Accès à distance aux systèmes d'information du CHU

Les accès à distance aux SI du CHU (accès dits « nomades ») doivent être réalisés via l'usage de réseaux privés virtuels (VPN) de confiance. Les accès distants par des tiers se font uniquement via la plateforme de télémaintenance « IPDIVA ».

12.3.15 – PDT-NOMAD-PAREFEU : Pare-feu local

Un pare-feu local conforme aux directives nationales (ANSSI) doit être installé sur les postes nomades.

12.3.16 – PDT-NOMAD-STOCK : Stockage local d'information sur les postes nomades

Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé (version de TRUECRYPT validée par l'ANSSI).

12.3.17 – PDT-NOMAD-FILT : Filtre de confidentialité

Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité doit être fourni et être positionné sur l'écran dès lors que le poste est utilisé en dehors du CHU.

12.3.18 – PDT-NOMAD-DESACTIV : Désactivation des interfaces de connexion sans fil

Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 3G...), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être définies et appliquées. Les interfaces sans fil ne doivent être activées qu'en cas de besoin.

Sécurisation des imprimantes et copieurs multifonctions**12.3.19 – PDT-MUL-DURCISS : Durcissement des imprimantes et copieurs multifonctions**

Les imprimantes et copieurs multifonctions hébergés au CHU doivent faire l'objet d'un durcissement en termes de sécurité : changement des mots de passe initialement fixés par le « constructeur », désactivation des interfaces réseau inutiles, suppression des services inutiles, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible, configuration réseau statique.

12.3.20 – PDT-MUL-SECNUM : Sécurisation de la fonction de numérisation

Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés au CHU doit être sécurisée. Les mesures de sécurité suivantes doivent notamment être appliquées : envoi de documents uniquement à destination d'une adresse de messagerie interne au CHU.

Sécurisation de la téléphonie**12.3.21 – PDT-TEL-MINIM : Sécuriser la configuration des autocommutateurs**

Les autocommutateurs doivent être maintenus à jour au niveau des correctifs de sécurité. Leur configuration doit être durcie. La définition et l'affectation des droits d'accès et des privilèges aux utilisateurs (transfert départ-départ, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé, etc.) doivent faire l'objet d'une attention particulière. Une revue de la programmation téléphonique doit être organisée périodiquement.

12.3.22 – PDT-TEL-CODES : Codes d'accès téléphoniques

Il est nécessaire de sensibiliser les utilisateurs au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.

Contrôles de conformité**12.3.23 – PDT-CONF-VERIF : Utiliser des outils de vérification automatique de la conformité**

Un outil de vérification régulière de la conformité des éléments de configuration des postes de travail doit être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration.

12.4 SÉCURITÉ DU DÉVELOPPEMENT DES SYSTÈMES

Les exigences relatives à la sécurité des développements du système d'information sont décrites ci-après :

Prise en compte de la sécurité dans le développement des SI

12.4.1 – DEV-INTEGR-SECLOC : Intégrer la sécurité dans les développements locaux

Toute initiative locale de développement informatique doit respecter les exigences nationales en matière de SSI, concernant la prise en compte de la sécurité dans les projets et les développements informatiques. Un document décrit la prise en compte de la sécurité dans les projets.

12.4.2 – DEV-SOUS-TRAIT : Intégrer des clauses de SSI dans les contrats de sous-traitance de développement informatique

Lors de l'écriture d'un contrat de sous-traitance de développement, plusieurs clauses relatives à la SSI doivent être intégrées :

- Formation obligatoire des développeurs sur le développement sécurisé et sur les vulnérabilités classiques ;
- Utilisation obligatoire d'outils permettant de minimiser les erreurs introduites durant le développement (outils gratuits d'analyse statique de code, utilisation de bibliothèques réputées pour leur sécurité, etc.) ;
- Production de documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement, etc.) ;
- Respect de normes de développement sécurisé, qu'elles soient propres au développeur, publiques ou propres au commanditaire ;
- Obligation pour le prestataire de corriger, dans un temps raisonnable et pour un prix défini, les vulnérabilités introduites durant le développement et qui lui sont remontées, en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation.

Prise en compte de la sécurité dans le développement des logiciels

12.4.3 – DEV-FUITES : Limiter les fuites d'information

Les fuites d'informations techniques sur les logiciels utilisés permettent aux attaquants de déceler plus facilement d'éventuelles vulnérabilités. Il est impératif de limiter fortement la diffusion d'informations au sujet des produits utilisés, même si cette précaution ne constitue pas une protection en tant que telle.

12.4.4 – DEV-LOG-ADHER : Réduire l'adhérence des applications à des produits ou technologies spécifiques

Le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. En phases de conception et de spécification technique, il est nécessaire de s'assurer que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent. En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent. En plus du maintien en condition de sécurité propre à l'application, il est donc nécessaire de pouvoir faire évoluer son environnement pour garantir sa sécurité dans la durée.

12.4.5 – DEV-LOG-CRIT : Instaurer des critères de développement sécurisé

Une fois passées les phases de définition des besoins et de conception de l'architecture applicative, le niveau de sécurité d'une application dépend fortement des modalités pratiques suivies lors de sa phase de développement.

12.4.6 – DEV-LOG-CYCLE : Intégrer la sécurité dans le cycle de vie du logiciel

La sécurité doit être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

12.4.7 – DEV-LOG-WEB : Améliorer la prise en compte de la sécurité dans les développements web

Les développements Web (et les développements en PHP en particulier) font l'objet de problèmes de sécurité récurrents qui ont conduit à la constitution de référentiels de sécurité.

Ces référentiels ont pour objectif de fixer des REGLES DE BONNES PRATIQUES à l'usage des développeurs. Ce sont des règles d'ordre générique ou pouvant être spécifiques à un langage (PHP, ASP, NET, etc.).

12.4.8 – DEV-LOG-PASS : Calculer les empreintes de mots de passe de manière sécurisée

Lorsqu'une application doit stocker les mots de passe de ses utilisateurs, il est important de mettre en œuvre des mesures permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute, etc.

Sécurisation des applications à risques**12.4.9 – DEV-FILT-APPL : Mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque**

Devant les applications à risques, il est recommandé de faire usage d'une solution tierce de filtrage applicatif.

13 ARCHITECTURE DES SI

Les exigences relatives à la sécurisation des archives du système d'information sont décrites ci-après :

13.1 Architecture sécurisée des centres informatiques

13.1.1 – ARCHI-HEBERG : Principes d'architecture de la zone d'hébergement

D'une manière générale, l'architecture des infrastructures des centres informatiques est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité. Le principe de défense en profondeur doit être respecté, en particulier par la mise en œuvre successive de « zones démilitarisées » (DMZ), d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.

13.1.2 – ARCHI-STOCKCI : Architecture de stockage et de sauvegarde

Le réseau de stockage/sauvegarde pour les besoins des centres informatiques repose sur une architecture dédiée à cet effet.

14 EXPLOITATION DES SI

Les exigences relatives à l'exploitation sécurisée du système d'information sont décrites ci-après :

14.1 Protection des informations sensibles

14.1.1 EXP-PROT-INF : Protection des informations sensibles en confidentialité et en intégrité

Des mesures doivent être mises en œuvre afin de garantir la protection des informations sensibles en confidentialité et en intégrité. A défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées à l'aide d'un moyen de chiffrement labellisé.

14.2 Surveillance et configuration des ressources informatiques

14.2.1 – EXP-TRAC : Traçabilité des interventions sur le système

Les interventions de maintenance sur les ressources informatiques du CHU doivent être tracées par le service informatique, et ces traces doivent être accessibles au RSSI durant au moins un an.

14.2.2 – EXP-CONFIG : Configuration des ressources informatiques

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

14.2.3 – EXP-DOC-CONFIG : Documentation des configurations

La configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.

14.3 Gestion des autorisations et contrôles d'accès logique aux ressources

14.3.1 – EXP-ID-AUTH : Identification, authentification et contrôle d'accès logique

L'accès à toute ressource non publique doit nécessiter une identification et une authentification individuelle de l'utilisateur. Dans le cas de l'accès à des données sensibles, des moyens d'authentification forte doivent être utilisés. A cette fin, l'usage d'une carte à puce doit être privilégié. Le contrôle d'accès doit être géré et s'appuyer sur un processus formalisé en cohérence avec la gestion des ressources humaines.

14.3.2 – EXP-DROITS : Droits d'accès aux ressources

Après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes suivants: besoin d'en connaître (chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès), moindre privilège (chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui).

14.3.3 – EXP-PROFILS : Gestion des profils d'accès aux applications

Les applications manipulant des données sensibles doivent permettre une gestion fine par profils d'accès. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

14.4 Processus d'autorisation

14.4.1 – EXP-PROC-AUTH : Autorisations d'accès des utilisateurs

Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI, doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ du personnel.

14.4.2 – EXP-REVUE-AUTH : Revue des autorisations d'accès

Une revue des autorisations d'accès doit être réalisée annuellement sous le contrôle du RSSI, le cas échéant avec l'appui du référent métier concerné.

14.5 Gestion des identifiants

14.5.1 – EXP-CONF-AUTH : Confidentialité des informations d'authentification

Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des données sensibles.

14.5.2 – EXP-GEST-PASS : Gestion des mots de passe

Les utilisateurs ne doivent pas stocker leurs mots de passe en clair (par exemple dans un fichier) sur leur poste de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.

14.5.3 – EXP-INIT-PASS : Initialisation des mots de passe

Chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique. Si les circonstances l'imposent, un mot de passe plus simple mais à usage unique peut être envisagé.

14.5.4 – EXP-POL-PASS : Politiques de mots de passe

Les règles de gestion et de protection des mots de passe donnant accès aux applications et infrastructures du CHU, doivent être respectées. Un document spécifique, décrit la politique de mots de passe applicable au CHU.

14.5.5 – EXP-CERTIFS : Utilisation de certificats électroniques

L'utilisation de certificats électroniques doit respecter les règles édictées par le RGS.

14.5.6 – EXP-QUAL-PASS : Contrôle systématique de la qualité des mots de passe

Des moyens techniques permettant d'imposer la politique de mots de passe (par exemple pour s'assurer du respect de l'éventuelle obligation relative à l'usage de caractères spéciaux) doivent être mis en place. A défaut, un contrôle périodique des paramètres techniques relatifs aux mots de passe doit être réalisé.

14.6 Gestion des authentifications d'administration

14.6.1 – EXP-SEQ-ADMIN : Séquestre des identifiants « administrateur »

Les authentifiant permettant l'administration des ressources des SI doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. L'authentifié doit être informé de l'existence de ces opérations de gestion, de leurs finalités et limites. Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit. Les informations d'authentification bénéficiant d'un moyen de protection physique (notamment carte à puce) n'ont, par défaut, pas besoin d'être l'objet d'opérations de séquestre de la part d'autres personnels que l'authentifié lui-même.

14.6.2 – EXP-POL-ADMIN : Politique de mots de passe « administrateur »

Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.

14.6.3 – EXP-DEP-ADMIN : Gestion du départ d'un administrateur des SI

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

14.7 Administration des systèmes

14.7.1 – EXP-RESTR-DROITS : Restriction des droits

Sauf exception dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droits d'administration.

14.7.2 – EXP-PROT-ADMIN : Protection des accès aux outils d'administration

L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès.

14.7.3 – EXP-HABILIT-ADMIN : Habilitation des administrateurs

L'habilitation des administrateurs s'effectue selon une procédure validée par l'autorité d'homologation. Le nombre de personnes habilitées pour des opérations d'administration doit être connu et validé par le RSSI.

14.7.4 – EXP-GEST-ADMIN : Gestion des actions d'administration

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

14.7.5 – EXP-SEC-FLUXADMIN : Sécurisation des flux d'administration

Les opérations d'administration sur les ressources locales du CHU doivent s'appuyer sur des protocoles sécurisés. Un réseau dédié à l'administration des équipements, ou au moins un réseau logiquement séparé de celui des utilisateurs, doit être utilisé. Les postes d'administrateurs doivent être dédiés et ne doivent pas pouvoir accéder à Internet.

14.7.6 – EXP-CENTRAL : Centraliser la gestion du système d'information

Afin de gérer efficacement un grand nombre de postes d'utilisateurs, de serveurs ou d'équipements réseau, les administrateurs doivent utiliser des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur le système d'information.

14.7.7 – EXP-SECX-DIST : Sécurisation des outils de prise de main à distance

La prise de main à distance d'une ressource informatique locale ne doit être réalisable que par les agents autorisés par l'équipe locale chargée des SI, sur les ressources informatiques de leur périmètre. Des mesures de sécurité spécifiques doivent être définies et respectées.

14.8 Administration des domaines

14.8.1 – EXP-DOM-POL : Définir une politique de gestion des comptes du domaine

Une politique explicite de gestion des comptes du domaine doit être documentée.

14.8.2 – EXP-DOM-PASS : Configurer la stratégie de mots de passe des domaines

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

14.8.3 – EXP-DOM-NOMENCLAT : Définir et appliquer une nomenclature des comptes du domaine

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

14.8.4 – EXP-DOM-RESTADMIN : Restreindre au maximum l'appartenance aux groupes d'administration du domaine

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

14.8.5 – EXP-DOM-SERV : Maîtriser l'utilisation des comptes de service

Les comptes de service ont la particularité d'avoir généralement leurs mots de passe inscrits en dur dans des applications ou dans des systèmes. Afin de pouvoir être en mesure de changer ces mots de passe en urgence, il est nécessaire de maîtriser leur utilisation.

14.8.6 – EXP-DOM-LIMITSERV : Limiter les droits des comptes de service

Les comptes de service doivent faire l'objet d'une restriction des droits, en suivant le principe du moindre privilège.

14.8.7 – EXP-DOM-OBSOLETE : Désactiver les comptes du domaine obsolètes

Il est nécessaire de désactiver immédiatement, voire de supprimer, les comptes obsolètes, que ce soient des comptes d'utilisateur (administrateur, de service ou utilisateur standard) ou des comptes de machine.

14.8.8 – EXP-DOM-ADMINLOC : Améliorer la gestion des comptes d'administrateur locaux

Afin d'empêcher la réutilisation des empreintes d'un compte utilisateur local d'une machine à une autre, il faut soit utiliser des mots de passe différents pour les comptes locaux d'administration, soit interdire la connexion à distance via ces comptes.

14.9 Envoi en maintenance et mise au rebut

14.9.1 – EXP-MAINT-EXT : Maintenance externe

Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique. Les opérations de chiffrement doivent faire appel à des produits qualifiés. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.

14.9.2 – EXP-MIS-REB : Mise au rebut

Lorsqu'une ressource informatique est amenée à quitter définitivement le CHU, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies par l'ANSSI.

14.10 Lutte contre les codes malveillants

14.10.1 – EXP-PROT-MALV : Protection contre les codes malveillants

Des logiciels de protection contre les codes malveillants, appelés communément antivirus, doivent être installés sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail du CHU. Ces logiciels de protection doivent être distincts pour ces trois catégories au moins, et le dépouillement de leurs journaux doit être corrélé.

14.10.2 – EXP-GES-ANTIVIR : Gestion des événements de sécurité de l'antivirus

Les événements de sécurité de l'antivirus doivent être remontés pour analyse statistique et gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

14.10.3 – EXP-MAJ-ANTIVIR : Mise à jour de la base de signatures

Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail par un dispositif géré par le domaine Infrastructure.

14.10.4 – EXP-NAVIG : Configuration du navigateur internet

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

14.11 Mise à jour des systèmes et des logiciels

14.11.1 – EXP-POL-COR : Définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité

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

14.11.2 – EXP-COR-SEC : Déploiement des correctifs de sécurité

Les correctifs de sécurité des ressources informatiques locales doivent être déployés régulièrement, par l'équipe du Domaine Infrastructure chargée des SI.

14.11.3 – EXP-OBSOLET : Assurer la migration des systèmes obsolètes

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

14.11.4 – EXP-ISOL : Isoler les systèmes restants

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

14.12 Journalisation

14.12.1 – EXP-JOUR-SUR : Journalisation des alertes

Chaque système doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité. Ces traces doivent être conservées de manière sûre.

14.12.2 – EXP-POL-JOUR : Définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces

Une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie par le RSSI, validée par l'autorité qualifiée, et mise en œuvre. Le niveau de sécurité d'un système d'information dépend en grande partie de la capacité de ses exploitants et administrateurs à détecter les erreurs, dysfonctionnements et tentatives d'accès illicites survenant sur les éléments qui le composent.

14.12.3 – EXP-CONS-JOUR : Conservation des journaux

Les journaux des événements de sécurité doivent être conservés sur douze mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

14.13 Gestion dynamique de la sécurité

14.13.1 – EXP-GES-DYN : Gestion dynamique de la sécurité

L'équipe en charge de la SSI doit procéder, notamment via l'analyse des journaux, à la surveillance des comportements anormaux au sein du système d'information, et à la surveillance des flux d'entrée et de sortie du système d'information.

14.14 Gestion des matériels informatiques fournis à l'utilisateur

14.14.1 – EXP-MAIT-MAT : Maîtrise des matériels

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

14.14.2 – EXP-PROT-VOL : Rappel des mesures de protection contre le vol

Les postes fixes bénéficient des mesures de protection physique offertes au titre de la directive de sécurité physique de la présente PSSI. Chaque utilisateur doit veiller à la sécurité des supports amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr. Il est recommandé de chiffrer les données contenues sur ces supports. Les supports contenant des données sensibles doivent être stockés dans des meubles fermant à clef.

14.14.3 – EXP-DECLAR-VOL : Déclarer les pertes et vols

Toute perte ou vol d'une ressource d'un système d'information doit être déclarée au RSSI.

14.14.4 – EXP-REAAFFECT : Réaffectation de matériels informatiques

Une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être mise en place et validée par le RSSI. Elle doit définir les conditions de recours à un effacement des données.

14.15 Nomadisme

14.15.1 – EXP-NOMAD-SENS : Déclaration des équipements nomades aptes à traiter des informations sensibles

L'autorité d'homologation du SI valide les usages possibles des équipements nomades vis-à-vis du traitement des informations sensibles ; les usages non explicitement autorisés sont interdits.

14.15.2 – EXP-ACC-DIST : Accès à distance au système d'information du CHU

Les utilisateurs distants doivent s'authentifier sur le réseau du CHU en utilisant une méthode conforme à l'annexe B3 du RGS.

14.16 Sécurité des ressources informatiques**14.16.1 – EXP-CI-OS : Systèmes d'exploitation**

Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque.

Une attention particulière doit être apportée aux comptes administrateurs.

14.16.2 – EXP-CI-TLP : Logiciels en tiers présentation

La mise en œuvre d'une configuration renforcée est obligatoire sur les logiciels déployés pour le tiers présentation (ex : serveur Web, Reverse Proxy).

14.16.3 – EXP-CI-LTA : Logiciels en tiers application

Des règles de développement sécurisé, et les configurations des logiciels en Tiers Application doivent être fixées et appliquées.

14.16.4 – EXP-CI-LTD : Logiciels en tiers données

Des règles très strictes (restrictions d'accès, interdictions de connexions, gestion des privilèges) s'appliquent aux logiciels en tiers données.

14.16.5 – EXP-CI-PROTFIC : Passerelle d'échange de fichiers

Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS...).

14.16.6 – EXP-CI-MESSTECH : Messagerie technique

Pour satisfaire les besoins d'exploitation et de supervision des infrastructures et des applications, une messagerie dite technique peut être déployée en zone de Back-office du centre informatique. Cette messagerie technique ne doit être en aucun cas utilisée directement par un utilisateur.

14.16.7 – EXP-CI-ADMIN : Flux d'administration

D'une manière générale, il convient de différencier deux types de flux d'administration : les flux d'administration de l'infrastructure (réservés aux agents du centre informatique) d'une part, les flux d'administration des applications métier (réservés à la direction métier) d'autre part. Il est recommandé d'attribuer les droits d'administration en respectant cette différenciation.

14.16.8 – EXP-CI-DNS : Service de noms de domaine – DNS technique

Dans le cas du déploiement d'un serveur de noms de domaines pour les besoins techniques internes au centre informatique, on utilisera les extensions sécurisées DNSSEC.

14.16.9 – EXP-CI-EFFAC : Effacement de support

Le reconditionnement et la réutilisation des disques durs pour un autre usage (ex : réattribution d'une machine/serveur) ne sont autorisés qu'après une opération d'effacement sécurisé des données.

14.16.10 – EXP-CI-DESTR : Destruction de support

La fin de vie d'un support ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur...) doit s'accompagner d'une opération de destruction avant mise au rebut.

14.16.11 – EXP-CI-TRAC : Traçabilité / imputabilité

Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les centres d'exploitation emploient une référence de temps commune (service NTP, Network Time Protocol).

14.16.12 – EXP-CI-SUPERVIS : Supervision

Un cloisonnement entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) doit être mis en place.

14.16.13 – EXP-CI-AMOV : Accès aux périphériques amovibles

L'accès aux supports informatiques amovibles fait l'objet d'un traitement adapté, plus particulièrement lorsqu'ils ont été utilisés pour mémoriser de l'information sensible ou lorsqu'ils sont utilisés pour des opérations d'exploitation.

14.16.14 – EXP-CI-ACCRES : Accès aux réseaux

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

14.16.15 – EXP-CI-AUDIT : Audit/contrôle

Le RSSI pilote des audits réguliers du système d'information relevant de sa responsabilité.

15 TRAITEMENT DES INCIDENTS

Les exigences relatives au traitement des incidents sur le système d'information sont décrites ci-après :

15.1 Chaînes opérationnelles

15.1.1 – TI-OPS-SSI : Chaînes opérationnelles SSI

Les chaînes opérationnelles des ministères concourent à l'effort national de cyber sécurité. Les alertes et les incidents sont gérés selon des procédures testées lors d'exercices. La coordination des compétences est organisée à l'échelon ministériel. Les situations d'urgence peuvent faire appel à des mesures définies préalablement dans le cadre des plans gouvernementaux.

15.2 Traitement des alertes de sécurité émises par les instances nationales

15.2.1 – TI-MOB : Mobilisation en cas d'alerte

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

15.3 Remontée des incidents de sécurité rencontrés

15.3.1 – TI-QUAL-TRAIT : Qualification et traitement des incidents

La chaîne fonctionnelle SSI est informée par la chaîne opérationnelle de tout incident de sécurité, et contribue si nécessaire à la qualification de l'incident et au pilotage de son traitement.

15.3.2 – TI-INC-REM : Remontée des incidents

Tout incident de sécurité, même apparemment mineur, dont l'impact dépasse ou est susceptible de dépasser le SI du CHU, fait l'objet d'un compte-rendu, via la chaîne SSI, au Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI) de l'ANSSI.

La remontée d'incidents par les chaînes opérationnelles ministérielles participe à la posture permanente de vigilance. Cette remontée est immédiate pour les incidents dont la portée est susceptible de dépasser à court terme le périmètre du CHU, et pour les incidents correspondant à des signalements spécifiques, notamment de la part de l'ANSSI.

16 REPRISE D'ACTIVITÉ

Les exigences relatives à la reprise d'activité du système d'information sont décrites ci-après :

16.1 Définition du PRA des SI

16.1.1 – PRA-LOCAL : Définition du PRA des SI

Le directeur des systèmes d'information ou le RSSI définit la structure et les attendus du plan de reprise d'activité des systèmes d'information permettant d'assurer effectivement, en cas de sinistre, la reprise d'activité.

16.2 Mise en œuvre du PRA des SI

16.2.1 – PRA-SUIVLOCAL : Suivi de la mise en œuvre du PRA des SI

Le RSSI s'assure de la bonne mise en œuvre des dispositions prévues dans le plan de reprise d'activité des systèmes d'information.

16.2.2 – PRA-PROC : Mise en œuvre des dispositions techniques et des procédures opérationnelles

Les équipes informatiques mettent en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la reprise des SI, en assurent la supervision au quotidien et la maintenance dans le temps.

16.2.3 – PRA-SAUVE : Protection de la disponibilité des sauvegardes

Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées.

16.2.4 – PRA-PROT : Protection de la confidentialité des sauvegardes

Les sauvegardes doivent être traitées de manière à garantir leur confidentialité et leur intégrité.

16.3 Maintien en conditions opérationnelles du PRA des SI

16.3.1 – PRA-EXERC : Exercice régulier du PRA des SI

Le RSSI organise des exercices réguliers, afin de tester le plan de reprise d'activité des systèmes d'information.

16.3.2 – PRA-MISAJOUR : Mise à jour du PRA des SI

Le RSSI assure le maintien à jour du plan de reprise d'activité des Systèmes d'Information.

17 CONFORMITÉ, AUDIT, INSPECTION, CONTRÔLE

Les exigences relatives à la conformité, l'audit, l'inspection et le contrôle du système d'information sont décrites ci-après :

17.1 Contrôles réguliers

17.1.1 – CONTR-SSI : Contrôles locaux

La conformité à la PSSI est vérifiée par des contrôles réguliers. Le RSSI du CHU conduit des actions d'évaluation de la conformité à la PSSI et contribue à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en œuvre.

18 PLAN D'ACTIONS

Les différentes règles définies dans la PSSI du CHU de Poitiers concourent à la diminution des risques identifiés dans l'analyse de risques. De cette analyse des risques découlent une liste de mesures à mettre en œuvre dans le but d'atténuer les risques identifiés. Ces mesures doivent être détaillées dans un plan d'actions.

19 OPERATEUR DE SERVICES ESSENTIELS

Du fait de son activité, le CHU de Poitiers est désigné par l'État comme Opérateur de Service Essentiel (OSE). Selon l'ANSSI, un OSE est défini comme suit :

« Un OSE est un opérateur tributaire des réseaux ou systèmes d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société. »

Un service essentiel correspond à trois critères :

- Φ *Ce service est essentiel au maintien d'activités sociétales ou économiques critiques ;*
- Φ *La fourniture de ce service est tributaire des réseaux et des systèmes d'information ;*
- Φ *Un incident sur ces réseaux et systèmes aurait un effet disruptif important sur la fourniture dudit service. »*

19.1 SYSTÈMES D'INFORMATION ESSENTIELS

Au CHU de Poitiers, un groupe de travail a été formé avec différents acteurs dans le but de désigner les systèmes d'information qui seront identifiés comme « essentiels ». Ce groupe de travail était formé du RSSI, du FSSI et de l'ANSSI.

Ces SIE ne sont pas décrits dans la version publique de la PSSI.

19.2 HOMOLOGATION DES SYSTÈMES D'INFORMATION ESSENTIELS

L'homologation de sécurité des Systèmes d'Information Essentiels permet d'intégrer la sécurité dans le cycle de vie des SIE, qu'il s'agisse de leur création ou maintien en conditions opérationnelles et en conditions de sécurité.

Chaque SIE fait l'objet de la constitution d'un dossier d'homologation, tenu à disposition de la seule Agence Nationale de la Sécurité des Systèmes d'Information. La composition du dossier d'homologation de chaque SIE est décrite dans le document « procédure-dossier-homologation-sie ».

20 GLOSSAIRE ET LISTE DES ABRÉVIATIONS

ABRÉVIATION	DÉFINITION
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
C.E	Comité d'Entreprise
CHT / GHT	Communauté/Groupement Hospitalière de Territoire
CHU	Centre Hospitalier Universitaire
DC	Data Center
DMP	Dossier Médical Patient
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HOP'EN	Hôpital Numérique Ouvert sur son Environnement (Programme Ministériel)
LAN / WAN	Local Area Network / Wide Area Network
OSE	Opérateur de Service Essentiel
NIS (Directive)	Directive Network & Information Security
NRBC	Risques Nucléaires, Radiologiques, Biologiques et Chimiques
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PMSSI	Politique Ministérielle de Sécurité des Systèmes d'Information
PRA	Plan de Reprise d'Activité
PSE	Plan de Sécurisation de l'Établissement
PSSI	Politique de Sécurité des Systèmes d'Information
PSSI MCAS	PSSI du Ministère Chargé des Affaires Sociales
PSSI-E	PSSI de l'État
RGS	Référentiel Général de Sécurité
RSSI	Responsable de la Sécurité du Système d'Information
RTC / GSM	Réseaux de téléphonie
SI	Système d'Information
SIE	Système d'Information Essentiel
SSI	Sécurité des Systèmes d'Information

21 ANNEXES

ANNEXE 1 : FONCTION SÉCURITÉ

FONCTION	NOM	CONTACT
RSSI	Pierre TAVEAU	rsi@chu-poitiers.fr
RSSI Adjoint	Nicolas ACQUIER	
Délégué à la Protection des Données	Pierre TAVEAU	dpo@chu-poitiers.fr

ANNEXE 2 : MÉTRIQUES D'ANALYSE DE RISQUES

ÉCHELLE DE NIVEAUX DE GRAVITÉ

La gravité est l'estimation de la hauteur des effets d'un événement redouté ou d'un risque. Elle représente ses conséquences.

VALEUR	PATIENT	SOCIAL & ORGANISATION	FINANCIER	RESPONSABILITE / JURIDIQUE	REPUTATION / IMAGE
1 - MINEURE	Gêne / inconfort pour un patient	Gêne ponctuelle dans la prise en charge d'usagers, ou l'activité Démotivation des acteurs / perte de temps	Perte financière sans impact significatif pour le responsable du traitement	Absence de plainte ou plaintes sans suite	Evènement peu ou pas médiatisé, sans effet ou effet négligeable sur l'image de l'organisme.
2 - SIGNIFICATIVE	Perte de chance pour un patient Effet indésirable limité et réversible sur un patient	- Surcharge de travail et/ou désorganisation modérée mais temporaire dans la prise en charge des usagers Conflit social - Interruption ou dégradation temporaire de certaines activités	Perte financière avec des impacts modérés pour le responsable du traitement	Contentieux	Dégradation passagère d'image ou de confiance dans l'acteur de santé ou le service offert
3 - IMPORTANTE	Perte de chance pour une population Soins inadéquats et/ou report de soins pour un patient entraînant une mise en danger immédiate du patient (atteinte sévère) et/ou une prolongation de la durée d'hospitalisation et/ou une réintervention avec ou sans perte de chances	- désorganisation importante et durable de l'activité entraînant une perte significative d'activité et/ou une replanification des soins ou un recours à des organismes tiers. Conflit social paralysant la structure	Perte financière avec des impacts importants pour le responsable du traitement	Atteinte à la vie privée d'un usager Condamnation pénale et/ou financière.	Perte d'image ou de confiance dans l'acteur de santé ou le service offert Mise en cause de la stratégie de l'organisme détenteur du système ou d'un organisme tiers
4 - CRITIQUE	Mise en danger d'une population / Menace du pronostic vital Atteinte irréversible ou décès d'un ou plusieurs patient(s).	Arrêt prolongé d'une part importante ou de toute l'activité. Arrêt du projet Fermeture de la structure	Perte financière mettant en cause la pérennité du responsable du traitement	Condamnation pénale et/ou financière Atteinte à la vie privée d'une population Risques judiciaires	Rejet définitif de l'acteur de santé ou du service offert Mise en cause de l'existence de l'organisme détenteur du système ou d'un organisme tiers

ÉCHELLE DE NIVEAUX DE VRAISEMBLANCE

La vraisemblance est l'estimation de la possibilité qu'un scénario de menace ou un risque, se produise. Elle représente sa force d'occurrence.

NIVEAU	LIBELLE	DESCRIPTION
1	EXCEPTIONNEL	Théoriquement possible, pas de cas rencontré par ailleurs, ou réalisable dans des conditions particulières, très difficiles à obtenir, nécessitant des moyens et compétences très importants. Evènement très rare s'il s'agit d'un accident (une occurrence sur une période de plusieurs dizaines d'années).
2	PEU PROBABLE	Cas déjà rencontré une ou plusieurs fois, rarement (une occurrence sur une période d'une dizaine d'années) pour un incident d'origine involontaire, ou réalisable dans des conditions difficiles pour une malveillance, avec nécessité de personnes organisées, très compétentes et disposant de moyens importants, ou malveillance présentant peu d'intérêt pour son auteur.
3	PLAUSIBLE	Cas rencontré assez fréquemment (une occurrence sur une période d'une à plusieurs années) par ailleurs, pouvant se produire avec probabilité pour un incident d'origine involontaire, ou réalisable dans des conditions occasionnelles pour une malveillance, par des personnes ou organisations dotées de moyens limités.
4	QUASI CERTAIN	Cas auquel le système est de toute façon confronté, fréquent (plusieurs fois par an), s'il s'agit d'un incident d'origine principalement involontaire ou réalisable facilement et avec un intérêt évident s'il s'agit d'une malveillance.

ÉCHELLE DE NIVEAU DE RISQUE

Cette échelle est définie par le tableau suivant qui combine le niveau de vraisemblance sur l'axe horizontal et le niveau de gravité sur l'axe vertical.

NIVEAU DE RISQUE	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

NIVEAU DE RISQUE	Exceptionnel	Peu probable	Plausible	Quasi certain
Mineur	Limité	Limité	Limité	Limité
Significatif	Limité	Limité	Modéré	Modéré
Important	Limité	Modéré	Fort	Fort
Critique	Limité	Modéré	Fort	Critique

Les risques étant identifiés comme ayant un « niveau de risque » inférieur ou égal à 4 sont désignés comme « limités » et sont assumés par le CHU de Poitiers.

Les risques étant identifiés comme ayant un « niveau de risque » désignés comme « modérés » et « forts » sont traités pour être réduits. Les risques de niveaux « fort » sont traités en priorité.

ANNEXE 3 : DOCUMENTS DE RÉFÉRENCE

- Référence n°1 : L'hygiène informatique en entreprise (ANSSI)
- Référence n°2 : Guide des professionnels de santé (CNIL)
- Référence n°3 : Programme Hôpital Numérique – Boîte à outils pour l'atteinte des prérequis –Fiches pratiques (DGOS)
- Référence n°3bis : Programme Hôpital Numérique – Boîte à outils : outil d'autodiagnostic et plan d'actions associé (fichier tableur Open Document ou Excel) (DGOS)
- Référence n°4 : Guide pratique pour la sécurité SI en établissement de santé – Fiches pratiques (DGOS)
- Référence n°5 : Recommandations de sécurité relatives aux mots de passe (ANSSI)
- Référence n°6 : Référentiels et guides pratique du corpus documentaire PGSSI-S
<http://esante.gouv.fr/pgssi-s/espace-publication>
- Référence n°6.1 : Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Structure sans approche SSI formalisée (voir Réf. n°6)
- Référence n°6.1bis : Annexe au canevas de PSSI pour les structures des secteurs sanitaire et médico-social : Couverture des règles de la PSSIE par les règles du canevas de PSSI (PGSSI-S) (voir Réf. n°6)
- Référence n°6.2 : Modèle de charte d'accès et d'usage du système d'information (voir Réf. n°6)
- Référence n°6.3 : Modèle de charte sécurité pour les personnels IT (voir Réf. n°6)
- Référence n°6.4 : Guide pratique « Plan de Continuité Informatique - Principes de base » (voir Réf. n°6)
- Référence n°6.5 : Guide Pratique « Règles pour les interventions à distance sur les Systèmes d'Information de Santé » (voir Réf. n°6)
- Référence n°6.6 : Guide Pratique « Règles pour les dispositifs connectés d'un Système d'Information de Santé » (voir Réf. n°6)
- Référence n°6.7 : Guide Pratique « Règles pour la mise en place d'un accès web au SIS pour des tiers » (voir Réf. n°6)
- Référence n°6.8 : Guide pratique spécifique pour la mise en place d'un accès Wifi (voir Réf. n°6)
- Référence n°6.9 : Guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé (voir Réf. n°6)
- Référence n°6.10 : Guide pratique « Règles de sauvegarde des Systèmes d'Information de Santé » (voir Réf. n°6)
- Référence n°6.11 : Référentiel d'identification des acteurs sanitaires et médico-sociaux (voir Réf. n°6)
- Référence n°6.12 : Référentiel d'authentification des acteurs de santé (voir Réf. n°6)
- Référence n°7 : Guide de l'externalisation « Externalisation et sécurité des systèmes d'information : maîtriser les risques » (ANSSI)
- Référence n°8 : TDBSSI – Guide d'élaboration de tableaux de bord de sécurité des systèmes d'information (ANSSI)
- Référence n°9 : Référentiel Général de Sécurité (RGS)
(<http://references.modernisation.gouv.fr/rgs-securite>)
- Référence n°10 : Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) – Version 1.0 (juillet 2014)
(<http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/>)
- Référence n°11 : Directive NIS (<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037444012>)