

# Référentiel de sécurité des systèmes d'information du CHU de BREST



## Références

Version du document	V 3.0
État	Validé

## Historique

Version	Date	Origine de la mise à jour	Rédigée par	Approuvé par
1.0	12/12/2019	Création du document	L. GUILLE	S. LAFFAY
1.1	14/02/2020	Modifications mineures	J. KEROULIN	S. LAFFAY
2.0	21/01/2022	Mise à jour	JS CHAVANNE	S. LAFFAY
3.0	24/08/2023	Mise à jour des exigences	JS CHAVANNE	J. DUTIL

## Documents associés

Titre du document	Version
Politique Générale de Sécurité des Systèmes d'Information de GHT de Bretagne Occidentale	1.0
Politique de Sécurité des Systèmes d'Information de GHT de Bretagne Occidentale	1.0

Classification du niveau de confidentialité du document		
<b>Public</b> <input checked="" type="checkbox"/>	Diffusable à tout public	
<b>Restreint</b> <input type="checkbox"/>	Périmètre	Diffusion interne ou uniquement à un groupe ou une équipe identifiée ou à des tiers contractualisés. Préciser en complément le périmètre.
<b>Confidentiel</b> <input type="checkbox"/>	Périmètre	Diffusion au propriétaire de la donnée et aux seules personnes habilitées internes à l'organisation. Préciser en complément le périmètre.
<b>Secret</b> <input type="checkbox"/>	Périmètre	Diffusion nécessite des dispositifs de chiffrement et de contrôle d'accès renforcés. Préciser en complément le périmètre.

## Table des matières

<b>1. INTRODUCTION.....</b>	<b>4</b>
<b>2. EXIGENCES DE SECURITE GENERALES .....</b>	<b>5</b>
2.1 EXIGENCES GENERALES SUR LES LOGICIELS.....	5
2.2 GESTION DES IDENTITES ET AUTHENTIFICATION .....	7
2.3 GESTION DES HABILITATIONS .....	9
2.4 TRAÇABILITE.....	11
2.5 PROTECTION DES SYSTEMES.....	12
2.6 CRYPTOGRAPHIE .....	13
2.7 MAINTENANCE ET TELEMANTENANCE.....	14
2.8 PROTECTION RELATIVE AUX ACCES WI-FI .....	16
2.9 PROTECTION DES DONNEES MEDICALES .....	16
<b>3. EXIGENCES SPECIFIQUES .....</b>	<b>18</b>
3.1 CAS DES DISPOSITIFS MOBILES .....	18
3.2 CAS DES DISPOSITIFS MEDICAUX CONNECTES (BIOMEDICAL) .....	19
3.3 CAS DES SERVICES HEBERGEES EN DEHORS DU SIH DU CHU (POUR TOUT OU PARTIE DE L'OBJET DU MARCHE) ET DES PRESTATIONS DE TYPE SAAS/IAAS & INFOGERANCE AU SEIN DU SIH .....	24
3.4 CAS DES FOURNISSEURS DE SERVICE DE DEVELOPPEMENT.....	27
<b>4. REFERENCES DOCUMENTAIRES .....</b>	<b>31</b>
<b>5. GLOSSAIRE .....</b>	<b>32</b>
<b>6. ANNEXE : DONNEES ATTENDUES DANS UN DAT .....</b>	<b>33</b>
<b>7. ANNEXE : DONNEES ATTENDUES DANS UN DOSSIER D'EXPLOITATION.....</b>	<b>34</b>
<b>8. ANNEXE : EXEMPLE DE MATRICE DE FLUX.....</b>	<b>35</b>
<b>9. ANNEXE : POLITIQUE GENERALE DE MOT DE PASSE AU CHU DE BREST.....</b>	<b>36</b>
<b>10. ANNEXE : EXEMPLE DE MATRICE RACI ENTRE LE CHU ET LE PARTENAIRE .....</b>	<b>37</b>

## 1. INTRODUCTION

Garantir la sécurité des systèmes d'information est primordial pour maintenir la confiance des patients et des professionnels dans les outils déployés au CHU de Brest. Par conséquent, les solutions numériques déployées au sein du Système d'Information Hospitalier (noté SIH) du CHU de Brest doivent :

- Satisfaire les exigences de sécurité informatique définies dans le présent **référentiel de sécurité du CHU de Brest**.
- Respecter les **préconisations en matière de sécurité de l'ANS** (Agence du Numérique en Santé), de **l'ANSSI** (Agence Nationale de la Sécurité des Systèmes de l'Information) et du **Ministère de la Santé et de la Prévention** (PSSI qui pourra être fournie sur demande).
- Respecter les exigences du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Respecter les exigences complémentaires propres à des systèmes critiques spécifiques.

**Les exigences de sécurité de ce référentiel sont obligatoires** et non négociables. Certaines exigences identifiées dans ce document peuvent être adaptées dans le CCTP.

Le chapitre **8.1** s'adresse au titulaire chargé d'administrer et/ou de maintenir de manière sécurisée une ou plusieurs solutions dans le SIH du CHU de Brest.

Le chapitre **9** s'adresse aux solutions intégrant un dispositif de connectivité Wi-Fi.

Le chapitre **11.1** s'adresse aux solutions intégrant un dispositif mobile.

Le chapitre **11.2** s'adresse aux solutions intégrant un dispositif connecté biomédical.

Les présentes exigences de sécurité seront intégrées dans la convention/le marché/le contrat conclu avec le CHU de Brest, le cas échéant et s'imposeront dans le cadre de son exécution.

Tous les documents référencés seront fournis au titulaire après la notification du marché et avant démarrage des services associés.

Le titulaire doit respecter les précautions mentionnées dans le guide de sécurité des données personnelles de la CNIL, édition 2018 et suivantes.

**Toutes les cases « description de la prise en charge » doivent être renseignées.** Si une règle n'est pas applicable la mention N/A est inscrite et doit être justifiée.

## 2. EXIGENCES DE SECURITE GENERALES

### 2.1 Exigences générales sur les logiciels

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.1.1	<p>Le titulaire s'engage à fournir la liste exhaustive des logiciels installés du projet.</p> <p>L'ensemble des éléments doivent être repris dans une cartographie qui doit être documentée (pré-requis, numéro de version, matrice de flux).</p> <p><i>[VOIR ANNEXE 3 – Exemple de matrice des flux]</i></p> <p>Le titulaire s'engage une fois le marché obtenu à rédiger avec le référent de l'établissement du CHU de Brest : le Document d'Architecture Technique (DAT) et le Document d'Exploitation (DEX).</p>		
2.1.2	<p>Le titulaire s'engage à n'installer et n'activer que les seuls logiciels nécessaires au bon fonctionnement du dispositif objet du marché.</p> <p>Si des logiciels complémentaires sont nécessaires ils devront être validés par l'établissement et présent dans le DAT.</p>		
2.1.3	<p>Le titulaire s'engage à utiliser et à mettre à jour les logiciels tiers utilisés par sa solution (comme les navigateurs ou les lecteurs PDF).</p>		
2.1.4	<p>Pour tout ce qui est fourni au titre de l'offre, le titulaire s'engage à acquérir et à concéder au CHU de Brest l'ensemble des licences d'utilisation nécessaires à son bon fonctionnement.</p> <p>Si nécessaire, il détaillera les conditions spécifiques ou exclusions.</p> <p>Ceci concerne l'ensemble des logiciels et couches logiques utilisées (OS, progiciels, BDD, télémaintenance...).</p>		
2.1.5	<p>Pour les logiciels libres, la conformité du logiciel est de la responsabilité du titulaire seul. Ils devront aussi respecter les exigences de sécurité décrites dans ce document.</p>		
2.1.6	<p>Pour les logiciels gratuits, la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité décrites dans ce document.</p>		
2.1.7	<p>Pour les logiciels de type SaaS (Software as a Service : logiciel hébergé), la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences générales de sécurité.</p>		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.1.8	Pour les applications web le titulaire s'engage à fournir avec l'offre un audit externe de sécurité de type top 10 de l'OWASP prouvant l'absence de faille de sécurité de niveau supérieur à 7 et de composant obsolète (sans maintenance de correctif de vulnérabilité de l'éditeur).		
2.1.9	Si la solution nécessite la mise en place de scripts, ils doivent être signés de préférence et ne pas comporter d'informations confidentielles en dur.		
2.1.10	Si la solution proposée entre dans le périmètre de sous-traitant du Règlement Général européen sur la Protection des Données (RGPD), le titulaire devra respecter ce règlement à date d'application et accepter des audits de vérification de conformité.		
2.1.11	Les applications ou services nécessitant un fonctionnement permanent, doivent être hébergés sur des machines ayant un système d'exploitation de type serveur et ne doivent pas dépendre d'une session utilisateur. Le fonctionnement en mode service est requis (des comptes gMSA pour les systèmes Windows et de service pour les autres systèmes peuvent être fournis par la DTSN).		
2.1.12	Seules des versions de système d'exploitation maintenues par l'éditeur en termes de mise à jour de sécurité doivent être installées.  Dans le cas où le CHU ne peut pas déployer de façon autonome des mises à jour, l'éditeur devra fournir un plan de mise à jour.  Le titulaire décrira tous les cas particuliers nécessitant une protection supplémentaire.		
2.1.13	Si la solution proposée doit être hébergée sur un serveur de l'établissement, elle doit être compatibles avec les prérequis fournis par la DTSN (précisés dans le CCTP).		
2.1.14	Si la solution proposée comporte des objets connectés (IOT), un rapport d'audit par un organisme spécialisé indépendant du titulaire est demandé avec la réponse.		
2.1.15	En cas de panne, le titulaire doit, avec le responsable métier du CHU, décrire les modalités de la procédure dégradée (avec une matrice de responsabilités).		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.1.16	<p>Le titulaire décrira en détail les procédures de secours et de gestion en mode dégradé, à savoir :</p> <ul style="list-style-type: none"> <li>• Les procédures de restauration des données</li> <li>• Les modalités de retour à l'état antérieur pour certains types de transactions</li> <li>• La méthodologie d'arrêt d'urgence</li> <li>• La méthodologie de reprise après incident</li> <li>• La méthodologie de vérification de l'intégrité de l'application</li> <li>• La méthodologie de vérification de l'intégrité des données</li> </ul>		

## 2.2 Gestion des identités et authentification

Le CHU de Brest a pris le parti d'établir le service d'annuaire de la société Microsoft (AD : Active Directory) en référentiel garant de l'unicité des comptes utilisateurs au sein du SIH.

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.2.1	<p>Le titulaire s'engage à fournir et maintenir un système destiné à répercuter le cycle de vie d'un utilisateur (arrivée, départ) dans son application.</p> <p>Ce système devra prendre la forme d'une interface entre l'application et le référentiel d'identité du CHU de Brest. Cette interface sera fournie et maintenue par le titulaire.</p> <p>Le titulaire s'engage, une fois le marché obtenu, à rédiger avec le référent de l'établissement du CHU de Brest, le document de spécifications fonctionnelles et techniques de l'interface.</p>		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.2.2	<p>Sauf disposition spécifique du CCTP, le CHU de Brest impose une compatibilité avec une authentification unique (Single Sign On) au travers de son système SSO utilisant une identité de domaine portée par les protocoles communément utilisés en environnement Windows (LDAPS). La politique de sécurité de l'authentification du CHU de Brest s'applique de fait aux comptes d'accès au système.</p> <p>Si une gestion de comptes utilisateurs et de mot de passe locale au système est spécifiée dans le CCTP, le système doit permettre d'imposer une politique de mots de passe robustes en accord avec la politique de sécurité du CHU de Brest (12 caractères pour le CHU selon le niveau de privilège comprenant majuscules, minuscules, chiffres et caractères spéciaux / délais de renouvellement / historisation) et respectant les recommandations de la CNIL et de l'ANSSI.</p> <p><u>[VOIR ANNEXE 2 : Politique de mots de passe au CHU de Brest.]</u></p>		
2.2.1	<p>Les mots de passe des comptes nécessaires à <b>l'administration</b> de la solution doivent respecter la politique de mot de passe des comptes à privilège du CHU à savoir un mot de passe complexe composé de 16 caractères minimum et ne pas être contenu dans un dictionnaire.</p>		
2.2.2	<p>L'utilisation du protocole NTLMv2 est tolérée pour les comptes non privilégiés, mais le protocole Kerberos est recommandé et la transition vers Kerberos doit être possible et disponible.</p>		

## 2.3 Gestion des habilitations

Le CHU de Brest a pris le parti de maintenir un référentiel central de gestion des habilitations sur son Système d'Information.

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.3.1	<p>Sauf disposition spécifique du CCTP, le CHU de Brest impose une gestion des habilitations à partir de son référentiel d'identités.</p> <p>Le titulaire s'engage une fois le marché obtenu à rédiger avec le référent du CHU le document de spécifications fonctionnelles et techniques de l'interface.</p>		
2.3.2	<p><b>Accès aux comptes privilégiés</b> : Les accès nécessitant des droits d'Administrateur de domaine ou supérieurs ne peuvent se faire à distance et doivent être effectués depuis les équipements de l'établissement. <u>Ces actions doivent être déléguées au personnel de l'établissement ou documentées et approuvées par l'établissement.</u></p>		
2.3.3	<p>Pour les applications web exposées sur internet et qui intégreraient une authentification et/ou une gestion des comptes :</p> <p>Les pages réservées à l'authentification et à la création de comptes doivent intégrer un dispositif de prémunition contre l'usage de robots (type test de défi-réponse).</p> <p>Des mécanismes empêchant de réutiliser des informations de connexion ou de session pour contourner l'authentification doivent être en place.</p> <p>L'interface d'administration doit être accessible seulement en interne.</p>		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	<p>Pour les applications web exposées sur Internet et qui intégreraient une authentification et/ou une gestion des comptes, les mécanismes d'authentification doivent être adaptés à la criticité des données</p> <p>Une authentification forte est notamment exigée pour l'accès à des données de santé par carte CPS ou équivalent et pour toutes données dites sensibles au sens du RGPD (sauf disposition contraire du CCTP qui conduirait le CHU de Brest à prendre en charge une authentification forte en préalable à l'accès à l'application objet du marché : cas d'un portail d'authentification en amont de l'application) en conformité avec l'arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé, applicable depuis juin 2022.</p>		
2.3.4	<p>Le processus d'authentification doit être, sauf disposition contraire du CCTP, compatible avec un service d'annuaire ou à un mécanisme SSO du type LDAP, SAML, OpenID.</p>		

## 2.4 Traçabilité

Les exigences fonctionnelles de traçabilité du CCTP peuvent être supérieures à celles citées ici d'une manière générale pour la sécurité.

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.4.1	La capacité (ou non) à tracer toutes les actions (y compris la consultation de données) doit être décrite et conforme à la réglementation liée au projet.		
2.4.2	Les accès utilisateurs (et administrateurs) seront tracés en réussite et en échec dans le système fourni.		
2.4.3	Dans le cadre de systèmes gérant des données à caractère personnel au sens du RGPD les traces de consultation et de modification sont obligatoires dans le système fourni.		
2.4.4	Les traces doivent pouvoir être épurée au-delà du temps légal de rétention notamment en conformité avec le RGPD.		
2.4.5	Le titulaire s'engage une fois le marché obtenu à formaliser à la demande du CHU de Brest le détail des traces générées, leur sécurisation et leur épuración.  Ces informations doivent se trouver dans un format de type Document d'Architecture Technique (DAT) et un Document d'Exploitation (DEX).		
2.4.6	Les traces produites sont un prérequis et devront être mise à disposition et accessibles gratuitement dans un format et un mode d'accès rendus possibles et décrits avec la fourniture du système par le titulaire (ATNA : format IHE, syslog, requête dans une base de données à fournir, fichier à décrire).		

## 2.5 Protection des systèmes

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.5.1	<p>Le titulaire s'engage à mettre en œuvre les dispositifs et paramétrages nécessaires pour prémunir ses systèmes contre les attaques virales et intrusives selon l'une des formes suivantes :</p> <ul style="list-style-type: none"> <li>Maintenir les composants à niveau en termes de sécurité et garantit une administration sécurisée intégrant a minima un antivirus mis à jour et un système d'exploitation ainsi que tous les composants mis à jour des correctifs de sécurité publiés par les éditeurs selon des modalités de qualification à décrire</li> <li>Intégrer ses dispositifs dans la démarche sécurité du CHU de Brest en installant l'antivirus du CHU ainsi que l'EDR ;</li> </ul> <p>De fait, en cas d'intrusion ou de contamination, le titulaire est responsable de la vulnérabilité de ses systèmes vis-à-vis des définitions virales et correctifs publics.</p>		
2.5.2	<p>Les exclusions d'analyses antivirales doivent être exceptionnelles. Elles ne peuvent se faire qu'uniquement sur des fichiers et non des dossiers (sauf dérogation du RSSI).</p> <p>Toutes les exceptions sont réalisées pour un temps limité de maximum 3 mois, afin d'avoir le délai pour lever l'exclusion (sauf dérogation du RSSI).</p> <p>Les condensats SHA256 devront être fournis.</p>		

## 2.6 Cryptographie

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.6.1	Dans le cas où la solution du titulaire utilise des algorithmes de chiffrement, ils doivent être à l'état de l'art et ne pas utiliser de suites cryptographiques obsolètes.		
2.6.2	Dans le cas d'applications web publiées sur Internet comme sur intranet, l'usage de TLS (avec suite cryptographique à l'état de l'art) est impératif (min TLS 1.2). Le titulaire pourra recourir à des certificats fournis par le CHU de BREST.		
2.6.3	Les données utiles à l'authentification doivent être chiffrées lors de leur communication et de leur stockage.		
2.6.4	De manière générale, si des techniques cryptographiques sont utilisées, elles doivent être conformes aux exigences de l' <a href="#">arrêté du 4 avril 2022 relatif à des moyens d'identification électronique immatériels mis à disposition des professionnels, personnes physiques des secteurs sanitaire, social et médico-social pour l'utilisation des services numériques en santé</a> , et au <a href="#">Référentiel Général de Sécurité (RGS)</a> .		
2.6.5	Si les logiciels fournis intègrent la gestion de données à caractère personnel au sens du RGPD au sein de systèmes de gestion de base de données standards (Microsoft SQL, Oracle, Mysql, ...) qui proposent le chiffrement des données, celui-ci devra être supporté par le titulaire et activable à décision du CHU de Brest. Les algorithmes et clefs de chiffrement seront conformes aux préconisations de la CNIL et au RGS.		

## 2.7 Maintenance et télémaintenance

Lorsqu'une télémaintenance est prévue par le titulaire, des règles strictes doivent être prises en compte :

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.7.1	<p>L'intervention de maintenance doit être encadrée entre le CHU de Brest et le titulaire, notamment concernant les engagements de chacun, les horaires d'accès, l'application des chartes et les modalités pratiques.</p> <p>Les personnels du titulaire devront signer la Charte de sécurité des fournisseurs qui rappelle les bonnes pratiques en vigueur.</p>		
2.7.2	<p>La connexion de télémaintenance doit se faire via les passerelles d'accès distants (VPN + Bastion) mises à disposition par la DTSN du CHU de Brest, conformément à sa politique de sécurité.</p> <p>L'accès à distance via le VPN permet une authentification renforcée (double facteur) et le bastion permet de tracer les actions réalisées par le titulaire sur le SIH.</p>		
2.7.3	<p>Les comptes des prestataires peuvent être activés de 8h à 18h les jours ouvrés. Le contact du titulaire au sein du CHU de Brest (ou la personne habilitée selon le protocole défini dans les conditions de la maintenance) peut activer le compte lors des besoins d'intervention sont identifiés.</p> <p>Les besoins aux plages d'horaires en dehors de 8h / 18h jours ouvrés doivent faire l'objet d'une demande de dérogation auprès du RSSI.</p>		
2.7.4	<p>Les besoins d'accès à la télémaintenance en 24/7 doivent être consignés dans le contrat entre le CHU de Brest et le titulaire avec une matrice de responsabilités.</p>		
2.7.5	<p>Si le titulaire ne souhaite pas passer par les équipements de sécurité du CHU (passerelle VPN SSL ainsi que le bastion), une demande de dérogation doit être effectuée auprès du RSSI en joignant une argumentation.</p>		
2.7.6	<p>Au niveau des postes de travail standard du CHU de Brest, aucun outil de prise en main à distance (PMAD) ne peut être installé ou exécuté. Le seul outil de PMAD autorisé est celui du CHU de Brest.</p>		
2.7.7	<p>Il est de la responsabilité du titulaire d'assurer la sécurité de sa plateforme d'intervention à distance (locaux, matériels, données, logiciels, habilitations), notamment la mise à jour des correctifs de sécurité et la mise en place d'un dispositif de protection contre les codes malveillants.</p>		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.7.8	Les données à caractère personnel ou technique (configuration des équipements) du CHU de Brest exploitées par les équipes de support chez le titulaire doivent être protégées et ne doivent pas être divulguées.		
2.7.9	Il est de la responsabilité du titulaire de sensibiliser son personnel à l'application des mesures de sécurité.		
2.7.10	Il est de la responsabilité du titulaire de connaître en toutes circonstances l'identité de toute personne qui se connecte ou s'est connectée sur la plateforme de télémaintenance et d'en assurer la traçabilité. Cette traçabilité pourra être communiquée sur demande du CHU de Brest.		
2.7.11	Il est de la responsabilité du titulaire de veiller à ce que toutes les informations résiduelles inutiles à l'issue d'une intervention soient supprimées (dont les outils ayant servi à réaliser des diagnostics).		
2.7.12	Le titulaire réalise un suivi permanent des incidents et vulnérabilités liés aux dispositifs connectés et met à disposition les correctifs et préventifs nécessaires dans les délais appropriés.		
2.7.13	Le titulaire s'engage à effectuer des tests de robustesse et de non-régression à chaque évolution du matériel ou du logiciel. Les impacts d'une défaillance qui serait néanmoins constatée seraient de la responsabilité du titulaire, la correction et la prise en charge des impacts à sa charge.  Des résultats de tests pourront être communiqués sur demande du CHU de Brest.		
2.7.14	Le titulaire doit informer le RSSI du CHU de Brest (voir contact en fin de document) de tout incident de sécurité concernant ses dispositifs connectés ou son SI d'entreprise pouvant impacter son matériel, le service ou les données du CHU de Brest.  Le titulaire s'engage à mobiliser les ressources nécessaires pour assurer le traitement de l'incident de sécurité sur les dispositifs déployés au CHU de Brest. Si l'incident concerne un traitement relatif RGPD les dispositions relatives au traitement des incidents s'appliqueront aussi.		
2.7.15	Le titulaire doit fournir un rapport détaillé pour chaque intervention effectuée (par simple mail).		

## 2.8 Protection relative aux accès Wi-Fi

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.8.1	Le chiffrement et l'intégrité des informations circulant sur le réseau doivent être assurés par la mise en place sur les équipements concernés du mécanisme WPA2 ou ultérieurs garantissant le plus haut niveau de sécurité (version de la norme IEEE 802.11i certifiée par la Wifi Alliance).		
2.8.2	Pour l'authentification, l'association de WPA2 ou supérieur (« WPA2 – Entreprise ») avec un serveur d'authentification 802.1X (Radius) par le biais du protocole EAP est demandée. Pour éviter la gestion redondante des comptes, le serveur devra s'appuyer sur l'annuaire centralisé de l'établissement.		

## 2.9 Protection des données médicales

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
2.9.1	Le titulaire et son personnel, sont soumis à un engagement de confidentialité conformément aux préconisations de la CNIL et au Code de la Santé Publique. Ces articles s'adressent notamment aux titulaires extérieurs.		

Article L1110-4 du Code de la Santé Publique

*[...] Excepté dans les cas de dérogation expressément prévus par la loi, ce secret (secret médical) couvre l'ensemble des informations concernant la personne venue à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé ainsi qu'à tous les professionnels intervenant dans le système de santé.*

Ref.	Règle de sécurité	Description de la prise en charge (OK/KO/NA)	Evaluation
2.9.2	En conséquence, notamment, les jeux de données fournies par le CHU de BREST sont strictement confidentiels et sont liés au secret professionnel.		
2.9.3	Un outil de pseudonymisation des données est souhaité. Cet outil doit permettre de banaliser les informations de la base de données ou bien des fichiers de données pour préserver le secret médical.		

Ref.	Règle de sécurité	Description de la prise en charge (OK/KO/NA)	Evaluation
2.9.4	<p>Si le centre de maintenance ou d'hébergement est en dehors du territoire national cela devra être précisé pour analyser les contraintes réglementaires associées au type de système à protéger selon la politique de sécurité de l'état et du ministère de rattachement.</p> <p>Le titulaire doit préciser les pays où sont réalisés les hébergements. Dans le cas d'hébergement hors communauté européenne les dispositions adaptées doivent être préalablement réalisées et validées par les autorités compétentes.</p>		
2.9.5	<p>Si des données de santé sont hébergées chez le titulaire ou un de ses sous-traitants celui-ci doit être agréé hébergeur de données de santé par l'ANS (ou toute commission compétente désignée par la réglementation).</p>		

### 3. EXIGENCES SPECIFIQUES

#### 3.1 Cas des dispositifs mobiles

Ref.	Règle de sécurité	Description de la prise en charge (OK/KO/NA)	Evaluation
3.1	Les dispositifs mobiles (smartphone, tablettes...) doivent être sous la responsabilité du titulaire. Par conséquent, les mises à jour de l'OS ainsi que les applications sont de son ressort.		
3.2	Les dispositifs mobiles doivent fonctionner avec des systèmes d'exploitation maintenus par les éditeurs.		
3.3	Le contrat doit prévoir le cas du renouvellement des matériels en fin du cycle de vie du système d'exploitation.		

## 3.2 Cas des dispositifs médicaux connectés (biomédical)

Les exigences contenues dans ce chapitre sont issues du [Guide Pratique des Exigences pour les dispositifs connectés d'un Système d'Information de Santé](#) de la PGSSI-S ainsi que du guide [Cybersécurité des Dispositifs Médicaux Intégrant du Logiciel Au cours de leur Cycle de Vie](#) de l'ANSM.

On entend par dispositif connecté **tout dispositif médical particulier connecté à un SI de Santé directement ou à distance** (par exemple via le réseau local ou Internet). Ce dispositif intègre des matériels (serveurs, périphériques, dispositifs électroniques spécifiques...), des logiciels (système d'exploitation, logiciels embarqué, micrologiciel) et des données (fichiers, bases de données, ...) et assure dans un processus de soin, une fonction de traitement médical, d'analyse médicale, de surveillance, de diagnostic ou de supervision.

### 3.2.1 Gestion des configurations

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
3.2.1.1	Le titulaire doit fournir dans sa documentation un DAT reprenant l'ensemble des composants matériels (serveurs, périphériques...), logiciels (versions des logiciels, systèmes d'exploitation, bases de données...) informatiques standards constituant le dispositif connecté ainsi que leurs principales caractéristiques, et leur architecture.		
3.2.1.2	Le titulaire doit préciser les modalités de partage des documents entre les équipements hors domaine et les équipements qui sont dans le domaine du CHU.		
3.2.1.3	Le titulaire doit identifier dans le DAT l'ensemble des spécifications portant sur le poste d'administration/utilisation du dispositif connecté (caractéristiques matérielles du poste, version du système d'exploitation, middleware et pilotes, services activés, périphériques...).		

### 3.2.2 Exploitation et communications

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
<b>Protection contre les codes malveillants</b>			
3.2.2.1	Les dispositifs connectés doivent comporter des moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants notamment dans le cas d'utilisation de supports amovibles.  Si le dispositif ne comporte pas de solution de type antivirus l'utilisation de support externe doit pouvoir être interdite ou contrôlée		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
3.2.2.2	<p>Les postes utilisateurs des dispositifs connectés doivent s'adapter aux systèmes de protection contre les codes malveillants (antivirus / EDR) du CHU de Brest ou comporter des moyens de sécurité permettant de détecter et d'éradiquer les menaces liées aux codes malveillants.</p> <p>Le fabricant doit fournir à l'établissement de santé la liste des outils de type antivirus / EDR avec lesquels ses logiciels et matériels sont compatibles.</p>		
Sécurité des réseaux			
3.2.2.3	<p>Le DAT du dispositif connecté doit comporter une matrice exhaustive des flux réseaux nécessaires à son intégration (types de protocoles, origine/destination des flux, plan d'adressage...).</p> <p><i>[VOIR ANNEXE 1 – Exemple de matrice des flux]</i></p>		
3.2.2.4	<p>Les flux doivent utiliser des protocoles chiffrés, même si ce sont des flux internes au SIH.</p> <p>Les protocoles doivent utiliser des suites cryptographiques à l'état de l'art.</p>		
3.2.2.5	<p>En cas de mise en œuvre de communications sans fil, le dispositif connecté doit être conforme aux exigences en vigueur dans les bonnes pratiques. Concernant le mode Wi-Fi, se référer aux exigences Wi-Fi du présent référentiel.</p>		
Sécurité des données			
3.2.2.6	<p>Afin de garantir l'intégrité des données, le dispositif connecté doit mettre en œuvre des protocoles de transmission adaptés permettant de vérifier l'équivalence des données reçues à celles émises.</p>		
3.2.2.7	<p>Les échanges de données du dispositif connecté doivent être conformes aux exigences de sécurité (notamment authentification et chiffrement) identifiées dans le Cadre d'Interopérabilité des SIS publié par l'ANS et aux recommandations du RGS.</p> <p>Le chiffrement des communications doit concerner tous les échanges depuis et vers le dispositif connecté avec toute autre ressource utile à son bon fonctionnement.</p>		
3.2.2.8	<p>L'accès aux fonctions d'export de données du dispositif connecté doit être limité à des personnes dûment habilitées.</p> <p>Les exports vers une destination hors du CHU de Brest, devront être contractuellement encadrés conformément au RGPD.</p>		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
Gestion des supports amovibles			
3.2.2.9	La fonction de démarrage du dispositif connecté à partir d'un support amovible doit être désactivée en fonctionnement nominal.		
Surveillance			
3.2.2.10	Le dispositif connecté doit comporter une fonction d'alerte locale permettant de signaler tout événement pouvant avoir un impact critique sur son fonctionnement.		
Journalisation			
3.2.2.11	<p>Le dispositif connecté doit comporter une fonction de journalisation locale permettant de conserver une trace des accès au dispositif connecté et de tout événement pouvant avoir un impact critique sur son fonctionnement en particulier les événements identifiés par l'exigence 2.4.2.</p> <p>Le titulaire doit indiquer dans son DAT les modalités de mise en œuvre de la journalisation en particulier les capacités de stockage de journaux du dispositif connecté et les recommandations en matière de sauvegarde des journaux.</p> <p>Il doit également fournir une procédure d'épuration automatique des journaux selon le délai légal de rétention.</p>		
Sauvegardes			
3.2.2.12	<p>Le dispositif connecté doit comporter une fonction de sauvegarde conforme aux exigences en vigueur. Si possible le dispositif doit permettre l'utilisation de VEEAM en vigueur au CHU de Brest.</p> <p>Le titulaire fournira dans son DAT les éléments suivants :</p> <ul style="list-style-type: none"> <li>la liste des données jugées vitales ;</li> <li>les différents types de sauvegarde (par exemple le mode hors ligne) ;</li> <li>la fréquence des sauvegardes ;</li> <li>la procédure d'administration et d'exécution des sauvegardes ;</li> <li>les informations de stockage et les restrictions d'accès aux sauvegardes ;</li> <li>les procédures de test de restauration ;</li> <li>la destruction des supports ayant contenu les sauvegardes.</li> </ul>		
Destruction des données lors des transferts de matériels informatiques			

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
3.2.2.13	<p>Le titulaire doit mettre en œuvre des fonctions de sécurité d'effacement des données conformes <a href="#">aux exigences en vigueur</a>.</p> <p>L'effacement des données devra être réalisé lors de la fin de vie du dispositif connecté, de sortie des locaux de l'établissement ou de fin de contrat. Une preuve de cet effacement devra être fournie.</p>		

### 3.2.3 Maîtrise des accès

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
3.2.3.1	Tout accès au système dispositif connecté nécessite une authentification préalable.		
3.2.3.2	<p>Le dispositif connecté doit comporter une fonction d'identification des utilisateurs sur la base de comptes nominatifs et une fonction d'authentification basée au minimum sur un mot de passe modifiable par les utilisateurs.</p> <p>Tous les mots de passe par défaut (y compris d'administration) doivent être changés lors de l'installation ou de la première connexion d'un utilisateur et être spécifiques à chaque client.</p>		
3.2.3.3	Les logiciels du dispositif connecté doivent offrir des fonctionnalités de verrouillage automatique en cas d'inactivité prolongée et de blocage (temporaires à minima) de comptes en cas de tentative d'accès non autorisé répétée.		
3.2.3.4	Les droits d'accès des utilisateurs doivent être organisés selon des rôles. La typologie de rôle sera fournie dans la proposition.		

### 3.2.4 Développement et maintenance des logiciels

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
3.2.4.1	<p>L'architecture générale du dispositif connecté et des logiciels développés doit être sans adhérence avec les briques système standards utilisées, en vue de faciliter les migrations de versions de logiciels.</p> <p>A défaut, le fournisseur doit assurer la compatibilité ascendante avec les évolutions des briques adhérentes.</p>		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
3.2.4.2	Le processus de développement doit respecter les bonnes pratiques de cybersécurité (notamment la correction des vulnérabilités liées aux débordements de tampon, erreurs internes des composants...).		
3.2.4.3	Le titulaire doit implémenter une fonction permettant de vérifier l'intégrité des logiciels lors de leur démarrage ou lors de leur mise à jour.		
3.2.4.4	Les modes de tests et de maintenance du dispositif connecté doivent être exclusifs du mode opérationnel.		
3.2.4.5	Le dispositif connecté doit disposer d'un mode dégradé (sécurisé) permettant son fonctionnement déconnecté du SIH avec une fonction de reprise des données lors du retour en mode nominal.		
3.2.4.6	Le titulaire doit proposer des solutions de restitution des données permettant une reprise de celles-ci par le CHU de Brest, notamment en cas de changement d'équipement, dans un format réutilisable par le client.		

### 3.2.5 Conformité

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
3.2.5.1	<p>Le titulaire doit réaliser une analyse de risques du système dispositif connecté et doit adapter les mesures de sécurité à mettre en œuvre dans ses produits au regard des risques résiduels.</p> <p>Il doit informer le RSSI du CHU de Brest de la méthode d'analyse de risques retenue, des risques couverts et des risques résiduels qui seront portés par le client. Il peut en outre préconiser des mesures de sécurité à mettre en œuvre par le CHU de Brest afin de réduire les risques résiduels identifiés dans le cadre des précautions d'usage du dispositif</p> <p>Enfin, il doit proposer au CHU de Brest et au référent Métier Biomédical en particulier, l'état des risques résiduels et leur acceptation.</p>		

### ***3.3 Cas des services hébergés en dehors du SIH du CHU (pour tout ou partie de l'objet du marché) et des prestations de type SaaS/IaaS & infogérance au sein du SIH***

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
3.3.1	Les services hébergés devront respecter les exigences de sécurité des réglementations nationales en vigueur (RGPD, directive NIS, arrêtés ministériels...)		
3.3.2	<p>Si le centre de maintenance ou d'hébergement est en dehors du territoire national cela devra être précisé dans le DAT pour analyser les contraintes réglementaires.</p> <p>Le titulaire doit préciser les pays où sont réalisés les hébergements. Dans le cas d'hébergement hors communauté européenne les dispositions adaptées doivent être préalablement réalisées et validées par le CHU de Brest et les autorités compétentes.</p>		
3.3.3	<p>Si des données de santé sont « hébergées » (cf sens donné par le CSP) chez le titulaire ou un de ses sous-traitants celui-ci doit être certifié hébergeur de données de santé conformément à l'article L 1111-8 du CSP.</p> <p>Pour le cadre spécifique de la recherche uniquement, des dispositions spécifiques de conformité au RGPD seront établies pour des hébergements hors UE.</p>		
3.3.4	Si la solution proposée entre dans le périmètre de sous-traitant au sens du RGPD le titulaire devra respecter ce règlement à date d'application et accepter des audits de vérification de conformité.		
3.3.5	<p>Si des données nominatives à caractère personnel font l'objet de traitement par le système, une conformité au RGPD est nécessaire et le titulaire devra démontrer le niveau de protection adapté à la criticité de ces données.</p> <p>Cette démonstration doit être intégrée dans les descriptions de la prise en charge des mesures concernées du présent document.</p>		
3.3.6	Le titulaire doit préciser les modalités d'accès aux journaux applicatifs par les personnels habilités du CHU de Brest.		

### 3.3.1 Concernant l'accès des utilisateurs du CHU de Brest au service hébergé

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
3.3.1.1	<p>Une authentification d'accès doit permettre aux utilisateurs d'accéder aux services avec un niveau de sécurité adapté aux données à protéger.</p> <p>Les utilisateurs pourront changer leur authentifiant (mot de passe ou moyen d'authentification). La confidentialité des mots de passe doit être garantie par l'hébergeur lors de son stockage (chiffré) et lors de sa saisie.</p> <p>Pour l'accès aux données de santé l'authentification devra être conforme aux exigences d'authentification forte de <a href="#">l'arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé.</a></p>		
	Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données. Le chiffrement utilisé doit être conforme au RGS.		
	Le titulaire doit remettre un compte et authentifiant pour audit à la demande du CHU de Brest et accepte que le CHU de Brest réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.		

### 3.3.2 Concernant la continuité du service hébergé

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	Le service doit respecter le taux de disponibilité décrit dans le CCTP.		

### 3.3.3 Concernant la réversibilité du service hébergé

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	Une copie exploitable des données (bases de données ou fichiers informatiques avec champs délimités et décrits) est transmise au CHU de Brest 3 mois avant la fin de ce contrat pour permettre la réalisation de tests de migration.		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	Une copie exploitable des données (bases de données ou fichiers informatiques avec champs délimités et décrits) est transmise au CHU de Brest en fin de contrat.		

### 3.3.4 Concernant la perte ou le renouvellement de certification d'hébergement de données de santé

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	Le titulaire certifié hébergeur de données de santé doit transmettre au CHU de Brest, dans les 10 jours, les résultats des audits de certification, de contrôle et de renouvellement.		

### 3.3.5 Exigences supplémentaires si la solution est hébergée au CHU de Brest mais administrée intégralement par le titulaire

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	Le titulaire doit s'engager à maintenir les composants à niveau en termes de sécurité et garantir une administration sécurisée intégrant prioritairement les dispositifs de lutte contre les codes malveillants du CHU de Brest. Sinon le titulaire fournira ces dispositifs et les modes de supervision.  Le système d'exploitation ainsi que tous les composants seront mis à jour des correctifs de sécurité publiés par les éditeurs selon des modalités de qualification à décrire.		
	L'accès depuis l'extérieur du CHU de Brest pour l'exploitation et la maintenance doivent respecter les conditions décrites au <b>paragraphe Maintenance et Télémaintenance (§ 2.7)</b> .		
	Pour tout type de traitement le titulaire doit remettre un compte et authentifiant pour audit à la demande du CHU de Brest et accepte que le CHU réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.		
	Les échanges avec l'extérieur du CHU de Brest doivent être sécurisés : utilisation de protocoles sécurisés, du filtrage et du contrôle par les équipements de sécurité. Le CHU se réserve le droit de tracer tout accès et action sur les systèmes installés dans son infrastructure).		

### 3.4 Cas des fournisseurs de service de développement

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	Les licences et modalités de la propriété intellectuelle relatifs au code source de l'appliquatif contractualisé doit être explicitées et définies dans le contrat de services avec le titulaire. Les délais de validité des licences doivent être acceptés par le CHU de Brest.		
	Les accords de séquestre concernant le code source du logiciel doivent être explicités et définis dans le contrat de service avec le titulaire afin de statuer sur des modalités de conservation du code source lors des différents jalons de développement.		
	Un plan de test doit être déterminé avec le fournisseur de services, comprenant : <ul style="list-style-type: none"> <li>a) Un programme détaillé des activités et des tests ;</li> <li>b) Les données d'entrée et les données de sorties attendues sous un ensemble de conditions ;</li> <li>c) Les critères pour évaluer les résultats ;</li> <li>d) La décision de mener des actions supplémentaires, si besoin.</li> </ul>		
	Des tests de sécurité doivent être menés par rapport à un ensemble d'exigences qui peuvent être exprimées comme fonctionnelles ou non fonctionnelles.  Il convient que les tests de sécurité incluent les tests : <ul style="list-style-type: none"> <li>a) des fonctions de sécurité : l'authentification des utilisateurs, les restrictions d'accès et l'utilisation de la cryptographie ;</li> <li>b) du codage sécurisé ;</li> <li>c) des configurations sécurisées, y compris celles des systèmes d'exploitation, des pare-feux et autres composants de sécurité.</li> </ul>		
	Le fournisseur de service, dans le cadre de la livraison de développement pour le CHU de Brest, doit présenter des preuves montrant que les tests suffisants ont été réalisés pour protéger le code source de la présence de contenus malveillants.  Le CHU pourra valider les preuves communiquées, et demander des compléments si celles-ci ne sont pas conformes avec ses attendus.		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	<p>Les développements du titulaire doivent respecter les principes de sécurité énoncés par l'organisme OWASP en vigueur, qui fournit une liste de dix domaines de vulnérabilités majeurs et les guides pratiques associés pour s'en prémunir :</p> <ul style="list-style-type: none"> <li>• A1 : Rupture de contrôle d'accès,</li> <li>• A2 : Défaillances cryptographiques,</li> <li>• A3 : Injection,</li> <li>• A4 : Conception non sécurisée,</li> <li>• A5 : Mauvaise configuration de sécurité,</li> <li>• A6 : Composants vulnérables et obsolètes,</li> <li>• A7 : Identification et authentification de mauvaise qualité,</li> <li>• A8 : Manque d'intégrité des données et du logiciel,</li> <li>• A9 : Carence des systèmes de contrôle et de journalisation,</li> <li>• A10 : Falsification de requêtes côté serveur</li> </ul>		
	<p>Les développeurs ne doivent en aucun cas utiliser du code provenant d'une source inconnue ou qui n'a pas été vérifiée (forums, internet, etc.). De plus, l'utilisation d'un code sous copyright est également prohibée, ou doit comporter une description contractuelle.</p>		
	<p>Le « codage en dur » d'identifiants dans le code source est prohibé.</p> <p>Les identifiants ne devant pas être « codés en dur » sont, de façon non exhaustive, les suivants :</p> <ul style="list-style-type: none"> <li>• Nom d'utilisateur,</li> <li>• Mot de passe,</li> <li>• Certificat électronique,</li> <li>• Numéro de jeton (token),</li> <li>• Numéro de téléphone.</li> </ul> <p>Les mesures de protection contre cette vulnérabilité sont décrites dans l'OWASP 2021 : A2 « Défaillances cryptographiques »</p>		
	<p>Le développement externalisé doit être supervisé et contrôlé par les équipes projet et les référents du CHU de Brest.</p> <p>En cas de développement externalisé, des contrats intégrant les bonnes pratiques de sécurité du présent clausier doivent être passés avec l'éditeur et le CHU de Brest.</p>		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	<p>L'application doit être développée et testée dans un environnement sécurisé, différent de la production.</p> <p>En développement « cycle en V » comme en méthode agile, l'équipe projet doit s'assurer que l'environnement de développement est bien distinct et cloisonné (dans la mesure du possible physiquement) par rapport aux environnements de préproduction/qualité et production.</p>		
	<p>Lors de l'utilisation de données de test en environnement de développement, un mécanisme d'anonymisation ou de pseudonymisation des données de production devrait être mis en place consistant à rendre peu probable, au mieux impossible, l'identification des personnes.</p>		
	<p>Les développeurs ne doivent pas publier le code source sur des forums ou sites internet spécialisés (ex : afin de demander des conseils).</p> <p>De plus, le code source doit être protégé dans un environnement sécurisé.</p> <p>Si la contribution à une communauté open source est nécessaire, le développeur doit demander autorisation au CHU de Brest.</p>		
	<p>Parce qu'ils peuvent contenir des informations qui peuvent être utilisées par des attaquants, les développeurs doivent supprimer tous les commentaires sensibles de leur code avant la mise en production de l'application.</p>		
	<p>Les tests de sécurité, pour les applications considérées comme sensibles (notamment manipulant de la donnée de santé nominative), doivent permettre de s'assurer que les exigences de sécurité ont été correctement appliquées.</p> <p>Lorsque la conception de l'application est terminée, des tests de sécurité doivent être réalisés avant sa mise en production (revue du code, test d'intrusion, scan de vulnérabilité, ...). Ces tests doivent également perdurer après la mise en production.</p>		
	<p>En complément des tests de sécurité, des audits techniques et tests d'intrusion devraient être planifiés avant une mise en production d'un applicatif lors des versions majeures.</p> <p>À la suite des tests de sécurité, le plan de traitement doit être validé afin de limiter la possibilité de découvrir de nouveaux risques ou <i>a minima</i> d'amoindrir leurs impacts s'ils sont inévitables.</p>		

Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
	<p>Le CHU de Brest, dans le cadre de la prestation de service contractualisé avec le fournisseur de service de développement, peut demander une fois par an un audit technique sur le développement engagé.</p> <p>Les modalités et les coûts de cet audit sont à la charge du CHU.</p> <p>Le CHU doit prévenir le fournisseur de services afin que celui-ci propose un planning de réalisation dans les 60 jours suivant la demande initiale.</p> <p>Le titulaire s'engage à corriger les vulnérabilités, dans un calendrier établi en accord avec le CHU.</p>		

#### 4. REFERENCES DOCUMENTAIRES

Guide Pratique Exigences pour les dispositifs connectés d'un Système d'Information de Santé - Politique Générale de Sécurité des Systèmes d'Information de Santé [PGSSI-S] - Novembre 2013 – v1.0

Disponible sur

[https://esante.gouv.fr/sites/default/files/media\\_entity/documents/Guide\\_Pratique\\_Dispositif\\_Connecte.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/Guide_Pratique_Dispositif_Connecte.pdf)

Guide d'hygiène informatique, ANSSI, version en vigueur.

Disponible sur <https://www.ssi.gouv.fr>

Norme internationale ISO/IEC 27001:2022 : Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences.

Disponible sur <https://www.iso.org>

Norme internationale ISO/IEC 27002:2022 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information.

Disponible sur <https://www.iso.org>

Prestataires d'administration et de maintenance sécurisées – Référentiel d'exigence, version 1.1 du 6 Octobre 2022

Disponible sur [https://www.ssi.gouv.fr/uploads/2022/10/anssi\\_pams\\_referentiel\\_v1.1\\_vfr.pdf](https://www.ssi.gouv.fr/uploads/2022/10/anssi_pams_referentiel_v1.1_vfr.pdf)

Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Disponible sur <https://eur-lex.europa.eu>

## 5. GLOSSAIRE

- ANS : Agence du Numérique en Santé
- BDD : Base de données
- CCTP : Cahier des Clauses Techniques Particulières
- CSP : Code de la Santé Publique
- DAT : Dossier d'Architecture Technique
- DEX : Dossier d'Exploitation
- DTSN : Direction de la Transformation et des Services Numériques
- EAP : Extensible Authentication Protocol
- EDR : Endpoint Detection and Response
- IEEE: Institute of Electrical and Electronics Engineers
- IoT : Internet of Things - Internet des objets
- LDAPS : Lightweight Directory Access Protocol Security
- NIS : Network and Information Security
- NTLM : New Technology LAN Manager
- OS : Operating System ou Système d'Exploitation
- OWASP : Open Web Application Security Project
- PMAD : Prise en Main à Distance
- PSSI : Politique de la Sécurité des Systèmes d'Information
- RGPD : Règlement Général pour la Protection des Données à caractère personnel
- RGS : Référentiel Général de Sécurité
- RSSI : Responsable de la Sécurité des Systèmes d'Information
- SAML : Security Assertion Markup Language
- SIH : Système d'Information Hospitalier
- SSO : Single Sign On - Authentification unique
- TLS : Transport Layer Security
- UE : Union Européenne
- WPA : Wi-Fi Protected Access

## **6. ANNEXE : DONNEES ATTENDUES DANS UN DAT**

*Ce sont des indications données à titre indicatif. Il peut y avoir des rubriques supplémentaires non citées.*

- **ARCHITECTURE CONCEPTUELLE**
  - Rappel des fonctionnalités du système d'information
  - Description macroscopique de l'environnement du système d'information
  - Exigences et contraintes
  - Contraintes d'environnement
    - Exigences en termes de qualité de services
    - Exigences en termes de sécurité
    - Exigences en volumétrie
- **ARCHITECTURE LOGIQUE**
  - Schéma d'architecture logique
  - Matrice de flux
- **ARCHITECTURE PHYSIQUE**
  - Plateforme de tests et de production
  - Serveur base de données
  - Poste client
- **SAUVEGARDES DONNEES ET APPLICATION**
  - Eléments à sauvegarder
  - Sauvegarde de la base de données
  - Sauvegarde de l'application
  - Scénario type de sauvegarde
- **RESTAURATIONS DONNEES ET APPLICATIONS**
  - Principes
  - Restauration des données en cas d'altération
  - Restauration de l'application en cas d'altération
  - Changement de serveur de données
  - Scénario type de restauration
  - Changement de serveur d'application

## 7. ANNEXE : DONNEES ATTENDUES DANS UN DOSSIER D'EXPLOITATION

*Ce sont des indications données à titre indicatif. Il peut y avoir des rubriques supplémentaires non citées.*

- **IDENTIFICATION ET CONNEXION**
  - Principe général
  - Paramétrage d'accès à la page de connexion
- **DEFINITION DES TACHES D'EXPLOITATION**
  - Serveurs applicatif
  - Serveurs de données
- **VERIFICATION DE L'ACCES A L'APPLICATION**
  - Modalités de démarrage et d'arrêt de l'application pour maintenance
  - Contrôle de la disponibilité de l'application
  - Accès à l'application en matière d'administration
- **PRINCIPAUX FICHIERS DE PARAMETRAGE DE L'APPLICATION**
  - Paramétrage du fichier d'accès a la base de données
  - Paramétrage du fichier XX.config
  - Paramétrage des images
  - Traitements batch standards de l'application
    - Descriptifs
    - Points de reprise sur incidents
    - Oordonnancements des batch et contraintes en termes d'exécution
- **INTERFACES**
  - Liste et paramétrage des interfaces
- **JOURNAUX**
  - Localisation des journaux et
  - Format des journaux (et encodage)

## 8. ANNEXE : EXEMPLE DE MATRICE DE FLUX

Date :

Type d'équipement	Nom de l'équipement	Service du CHU	SN	@MAC	IP SOURCE	IP DESTINATION	URL	PORT	PROTOCOLE	REMARQUE

Les colonnes en rouge sont obligatoires pour ouvrir les flux.  
Les colonnes en violet sont contextuelles.

## 9. ANNEXE : POLITIQUE GENERALE DE MOT DE PASSE AU CHU DE BREST

Pour les utilisateurs :

- Le mot de passe doit comporter au minimum **12 caractères**
- Le mot de passe doit comporter au minimum 3 des 4 types de caractères qui sont : majuscules, minuscules, chiffres, caractères spéciaux
- Durée de validité de **6 mois**
- Le mot de passe doit être différent des 11 derniers mots de passe
- Le compte se verrouille après 6 tentatives infructueuses de saisie de mot de passe
- En cas d'inactivité sur un poste durant 15 min, le pc se met en veille, et nécessite une ressaisie du mot de passe.

Pour les comptes d'administration :

- Le mot de passe doit comporter au minimum **16 caractères**
- Le mot de passe doit comporter au minimum 3 des 4 types de caractères qui sont : majuscules, minuscules, chiffres, caractères spéciaux
- Durée de validité de **2 ans**
- Le mot de passe doit être différent des 11 derniers mots de passe
- Le compte se verrouille après 6 tentatives infructueuses de saisie de mot de passe
- En cas d'inactivité sur un poste durant 15 min, le pc se met en veille, et nécessite une ressaisie du mot de passe.

## 10. ANNEXE : EXEMPLE DE MATRICE RACI ENTRE LE CHU ET LE PARTENAIRE

Un tableau « RASCI » décrit les responsabilités et le niveau d'implication avec les rôles suivants :

- **Réalise (R)** : la personne fait le travail et réalise les opérations
- **Autorise (A)** : la personne est l'unique décideur de la validité de la procédure
- **Supporte (S)** : la personne apporte un soutien à (R)
- **Consulté (C)** : la personne peut être sollicitée pour apporter des conseils
- **Informé (I)** : la personne doit être informée de l'évolution du projet

Logiciel : <<NOM DU LOGICIEL>>

---

	Editeur	CHU Brest – DTSN Infrastructure	CHU Brest – DTSN – Projet et application	CHU Brest – Service client
<b>Phase projet : Application</b>				
Expression du besoin métier			S	R
Expression des prérequis techniques		S	R	
Elaboration du cahier des charges			R	
Remise du Dossier d'Architecture Technique (DAT) qui répond au cahier des charges				
Installation (si on premise) ou remise des procédures d'installation				
Développement ou installation du ou des connecteurs (EAI/EDI)				
Remise de la documentation d'exploitation (DEX)				
Remise des procédures dégradées				
Tests et recette du logiciel dans l'environnement de test				
Tests et recette du logiciel dans l'environnement de production				
Mise à jour du logiciel métier				
<b>Phase projet : INFRASTRUCTURE</b>				
Gestion et ouverture de la télémaintenance				
Spécification infrastructure				
Mise en place infrastructure				
Mise à jour de l'OS				
Mise à jour du middleware				
Mise en place des procédures de sauvegardes du logiciel				
Mise en place des procédures de sauvegardes des données				
<b>VERIFICATION D'APTITUDE</b>				
<b>VERIFICATION SERVICE REGULIER</b>				

Phase de fonctionnement				
Support de premier niveau	<b>R</b>	S	S	
Support de deuxième niveau				
Astreinte hors JO	<b>N/A</b>	N/A	N/A	N/A
Mise à jour de l'OS				
Mise à jour du middleware				
Mise à jour du logiciel métier				
Sauvegardes du logiciel				
Sauvegardes des données				
Gestion et ouverture de la télémaintenance				