Sécurité informatique des équipements techniques – Exigences

Ce référentiel détaille les exigences de sécurité pour les équipements techniques connectables au réseau informatique. Il exprime le consensus du groupe d'experts « HIL » (Hospital Infosec Liaison), qui représente des hôpitaux de la santé publique des cantons suisses suivants : Fribourg, Genève, Tessin, Valais, Vaud.

Version 3.0

Juin 2015

Numéro de référence : HIL H.TEC:2015/v3.0 (F)

Table des matières

0.1 Historique des versions

Date	Auteur	Modifications	Version	Statut
2011-03-18	F. Calcavecchia (HUG)	HUG version 1.0	1.0	Final
2013-06-18	F. Calcavecchia (HUG)	HUG version 2.0	2.0	Final
2015-06-08	HIL (HUG, CHUV, EOC, FHVI, HFR, HVS)	Première version HIL validée	3.0	Validé

0.2 Approbations du référentiel

Institution, canton	Représentée au groupe HIL par	Date
HFR / Etat FR, Fribourg	A. Jordi, A. Müller	08.06.2015
HUG, Genève	F. Calcavecchia	08.06.2015
EOC, Tessin	M. Marazza	08.06.2015
HVS, Valais	M. Buri	08.06.2015
CHUV, Vaud	J. Kenaghan	08.06.2015
FHV / FHVI, Vaud	P. Cohen	08.06.2015

0.3 Termes et abréviations

Terme / abréviation	Signification dans le contexte du présent document
DSI	Direction du Système d'Information, soit le service informatique de l'hôpital
HIL	« Hospital Infosec Liaison », groupe d'experts en sécurité de l'information, provenant de plusieurs hôpitaux suisses. Le groupe HIL est l'auteur du présent document.
Hôpital	Selon le contexte dans lequel le terme apparaît dans le présent document, « l'hôpital » signifie l'institution (l'établissement de soins ou le groupe d'établissements) qui est responsable pour : (a) le projet d'acquisition de l'équipement, (b) l'exploitation et l'utilisation de l'équipement, et/ou (c) le service informatique et le réseau informatique. *[Ces responsabilités peuvent être clarifiées dans des documents annexes, si nécessaire, notamment dans le cas d'une structure d'organisation complexe.]*
IT Security Officer	Personne ou structure organisationnelle, désignée par l'hôpital pour valider ou refuser une éventuelle demande d'exception aux exigences de sécurité. Le titre officiel de cette fonction peut varier selon l'hôpital. *[Implicitement, un projet de mise en place d'un équipement technique nécessite un travail collaboratif en équipe pluridisciplinaire. Le partage des responsabilités entre les différents acteurs du projet peut dépendre de la structure de l'hôpital et de l'organisation spécifique du projet. Si nécessaire, les rôles de certains acteurs peuvent être clarifiés dans des documents annexes.]*
NDA	Non-Disclosure Agreement (Accord de confidentialité)
OS	Operating System (Système d'exploitation)
PACS	Picture Archiving and Communication System
P	Voir 2.2 Classification des exigences
Q	Voir 2.2 Classification des exigences
H.TEC.nn	Numéro de référence d'une exigence de sécurité pour les équipements techniques

1 Introduction

1.1 Contexte

Dans des domaines techniques tels que le biomédical ou la gestion des bâtiments, il est de plus en plus courant qu'un équipement technique soit capable de se connecter à un réseau informatique : par exemple, afin de communiquer avec des applications informatiques ou d'être accédé par un tiers externe.

Malheureusement, nous constatons que les bonnes pratiques de sécurité de l'information ne sont pas toujours respectées par ces équipements. Avec la connectivité croissante des équipements techniques, le milieu hospitalier perçoit une croissance du nombre d'incidents de sécurité liés à ces équipements : des infections, des fuites de données sensibles, etc.

Concernés par ces risques, plusieurs hôpitaux suisses ont décidé collectivement – sous le nom « *Hospital Infosec Liaison* » (HIL) – de formaliser dans le présent document un certain nombre d'exigences de sécurité applicables à tout **équipement technique susceptible d'être raccordé au réseau informatique**.

1.2 Définition

Est dénommé « **équipement technique** » tout dispositif associant des matériels, logiciels et composants de communication (réseau) utilisé dans l'hôpital, dans les domaines :

- du biomédical (dispositif médical assurant un processus de soin, une fonction de traitement médical, d'analyse médicale, de surveillance médicale, de diagnostic ou de supervision) ;
- des laboratoires d'analyse médicale, ou similaire ;
- de la gestion des bâtiments (Gestion Technique de Bâtiment, Gestion Technique Centralisée, détecteurs, onduleurs, systèmes de climatisation, vidéosurveillance, contrôles d'accès, etc.).

1.3 Utilisations du présent document

Les hôpitaux suisses sont libres d'utiliser le présent document à toute fin utile, notamment comme **référentiel** lors de la mise en place de nouveaux systèmes ou lors d'un audit.

Dans le cas d'un appel d'offres, ce document (ou une copie des exigences du chapitre 2 « Exigences techniques de sécurité ») fait généralement partie intégrante de l'appel d'offres et des documents contractuels. Les fournisseurs d'équipements techniques doivent alors impérativement se positionner sur chacune des exigences (qu'elle soit de caractère obligatoire ou non), en remplissant une liste de contrôle (« checklist ») fournie par l'hôpital. En cas d'absence de la checklist dûment remplie, l'hôpital se réserve le droit d'éliminer l'offre en question.

La checklist de l'hôpital peut s'inspirer de celle fournie comme modèle dans l'Annexe A, mais l'hôpital est libre de l'adapter à ses besoins et peut notamment ajouter des exigences et/ou des précisions supplémentaires.

1.4 Audience

Ce document est destiné :

- aux fournisseurs dans le cadre de consultations pour l'acquisition de nouveaux équipements techniques, en tant qu'annexe au cahier des charges,
- aux équipes internes de l'hôpital, en charge des acquisitions ou des contrats,
- aux équipes en charge de l'installation et de la configuration des équipements techniques,
- aux auditeurs.

2 Exigences techniques de sécurité

2.1 But des exigences

Ces exigences visent :

- d'une part, à sécuriser l'équipement technique contre des infections informatiques ou des attaques potentielles provenant du réseau de l'hôpital ou de l'extérieur ;
- d'autre part, à protéger le Système d'Information de l'hôpital contre les risques propres à l'équipement technique.

2.2 Classification des exigences

Les exigences détaillées ci-dessous sont catégorisées de la manière suivante :

- **P** = Critère prérequis : Exigence généralement considérée comme essentielle et incontournable. Dans le cadre d'un appel d'offres : l'hôpital se réserve le droit d'éliminer une offre non conforme, sans autre justification. Le caractère obligatoire est rappelé ci-après par un soulignement du numéro de référence et la couleur rouge (ex : H.TEC.8).
- **Q** = Critère de qualification : Caractéristique souhaitée ; bonne pratique de sécurité. Dans le cadre d'un appel d'offres: les précisions du fournisseur sont prises en compte dans l'évaluation de l'offre. Les exceptions ou les demandes de dérogation devront être justifiées (ex : contrainte induite par une application) et validées auprès du *IT Security Officer* désigné par l'hôpital.

2.3 Liste des exigences

RÉFÉRENCE	P / Q	MESURE DE SÉCURITÉ
2.3.1 Documentation		
H.TEC.1	P	**Documentation technique de l'équipement** Le fournisseur doit préciser et maintenir à jour dans son dossier technique (fourni à l'hôpital) la liste des logiciels installés (le système d'exploitation, les applications et tout autre composant significatif ou utile ?) en indiquant pour chacun l'éditeur, la licence, le numéro de version, et le niveau des correctifs (OS + Security patches). Le fournisseur doit également préciser et documenter de manière adéquate les services et ports réseau utilisés, notamment en écoute.
H.TEC.2	P	**Documentation architecture et exploitation** Le système doit être documenté. La documentation doit comprendre les dossiers détaillés d'architecture avec flux de données (e.g. HL7, DICOM, …), d'installation, d'exploitation et de maintenance. Ces documents seront soumis à l'approbation de la DSI avant raccordement du système au réseau.
2.3.2 Configuration de base		
H.TEC.3	Q	**Système d'exploitation standard** Dans le cas où l'hôpital devrait assurer l'administration et l'exploitation courante de l'équipement technique, ce dernier doit impérativement fonctionner sur la base de systèmes d'exploitation standardisés par la DSI (Direction du Système d'Information) de l'hôpital.
H.TEC.4	Q	**Surface d'exposition** Afin de réduire la surface d'exposition des composants de l'équipement technique directement exposé sur le réseau de l'hôpital, le fournisseur doit s'assurer que seuls les logiciels nécessaires au fonctionnement de l'équipement technique y sont installés. Tous les logiciels non requis doivent être désinstallés ou désactivés. Si des ports réseau sont en écoute, ceux-ci doivent correspondre à un besoin opérationnel validé par l'hôpital.
H.TEC.5	Q	**Versions du système d'exploitation supportées** Pour obtenir le droit de raccorder un nouvel équipement technique au réseau de l'hôpital, le fournisseur doit s'engager à suivre le cycle technique de montée de versions proposé par l'éditeur (ex : Microsoft) du système d'exploitation (ex : Windows) de l'équipement concerné. Un équipement technique raccordé au réseau de l'hôpital ne doit en aucun cas fonctionner sur un système d'exploitation qui n'est plus supportés par l'éditeur. (Par exemple, Windows XP n'est plus supporté par son éditeur, Microsoft, depuis avril 2014.) En cas d'impossibilité technique à suivre cette évolution du système d'exploitation, la DSI de l'hôpital pourra être amenée à isoler l'équipement du réseau principal ou à le déporter sur un autre réseau.

RÉFÉRENCE	P / Q	MESURE DE SÉCURITÉ
H.TEC.6	**Q**	**Gestion des correctifs de sécurité** Pour garantir la sécurité de son infrastructure, l'hôpital assure un processus d'application des correctifs de sécurité (patches) et des mises à jour des systèmes exploitation et des principaux logiciels en réponse aux alertes de sécurité. Par conséquent, pour les composants de l'équipement technique connectés au réseau de l'hôpital, le fournisseur doit valider et garantir le bon fonctionnement (ou proposer une évolution) de l'équipement avec les derniers correctifs de sécurité proposés par les éditeurs (du système d'exploitation et des autres logiciels standard potentiellement vulnérables) dans un délai maximum de 2 mois à compter de leur date de publication. En cas d'impossibilité à suivre cette évolution des correctifs de sécurité, la DSI de l'hôpital pourrait être amené à isoler l'équipement technique du réseau principal ou à le déporter sur un autre réseau.
H.TEC.7	**P**	**Gestion des données personnelles** Le fournisseur doit décrire les types de ***données personnelles*** qui sont stockées ou traitées par le système. Pour les systèmes qui conservent durablement des données personnelles identifiables (notamment celles des patients), cette description est nécessaire pour la validation du système par l'autorité compétente de l'hôpital, qui pourra exiger des compléments d'information ou des mesures de sécurité additionnelles. La validation du système est impérative avant la mise en service du système (ou de préférence, avant son acquisition). L'obtention de cette validation est usuellement de la responsabilité du chef de projet ou du demandeur du raccordement au réseau, avec le soutien du *IT Security Officer* désigné par l'hôpital.
2.3.3 Protection contre les malwares		
H.TEC.8	**P**	**Anti-malware** Sauf contrainte rédhibitoire, les composants de l'équipement technique exposés sur le réseau informatique doivent être protégés par une solution anti-malware validée par l'hôpital. Si la perte d'une homologation (par ex, marquage « CE ») est citée comme raison pour le manque de protection anti-malware, le fournisseur doit en apporter la preuve. Le cas échéant, le constructeur spécifiera les répertoires à exclure des activités de protection. Il précisera également les chemins d'exécution autorisés. A la place d'un antivirus classique qui requiert des mises à jour quotidiennes, les solutions de « whitelisting » permettant de certifier et contrôler l'intégrité du contenu logiciel d'un équipement sont acceptées.
H.TEC.9	**P**	**Mise à jour des signatures** Afin de bénéficier des dernières signatures et versions, l'antivirus doit impérativement se mettre à jour **quotidiennement** depuis un serveur central de référence de l'hôpital si ce dernier est d'accord de supporter cette configuration, ou à partir d'un serveur externe dans le cas contraire. Cette mise à jour doit être automatique. Pour les solutions basées sur du « white listing » ces mises à jour quotidiennes ne sont, par définition, pas requises.

RÉFÉRENCE	P / Q	MESURE DE SÉCURITÉ
H.TEC.10	P	**Contrôle des supports externes** Le fournisseur précisera si le fonctionnement de l'équipement technique nécessite l'utilisation de dispositifs de stockage externes (clé USB, disque externe ou autre), ainsi que la raison opérationnelle. Dans tous les cas, et afin de réduire le risque d'exécution de codes malveillants, les fonctions « autorun » d'exécution automatique des lecteurs de périphériques amovibles (y compris lecteurs de CD-ROM / DVD) doivent être désactivées sur l'équipement technique.
2.3.4 Accès réseau		
H.TEC.11	Q	**Authentification machine** Il est recommandé d'utiliser une méthode appropriée d'authentification machine, en favorisant notamment 802.1x. Les méthodes d'authentification machine supportées ou préconisées doivent être précisées.
H.TEC.12	Q	**Protocoles réseau sécurisés** Lorsqu'elles sont disponibles, les variantes sécurisées des protocoles de communication (SSH, SFTP, SSL…) doivent être favorisées, notamment pour les accès aux fonctions d'administration du système et pour les éventuels transferts de données patients. Il est en effet préférable que les communications soient chiffrées, même au sein de l'établissement. Les services équivalents non sécurisés (telnet, Rlogin, FTP…) sont alors impérativement désactivés.
H.TEC.13	P	**Double connexion réseau** Pour les équipements doublement interconnectés (notamment, d'une part au réseau de l'hôpital et d'autre part au réseau interne de l'équipement technique), les fonctions de routage ou pontage entre les deux interfaces doivent impérativement être désactivées.
H.TEC.14	P	**Connexions sans fil** Les communications entre les divers composants du système doivent impérativement se faire par les liaisons filaires. Les liaisons sans fil (par exemple, Wifi ou Bluetooth) sont interdites sauf validation spécifique par le *IT Security Officer* désigné par l'hôpital.
H.TEC.15	P	**Connexions externes** Pour les systèmes techniques qui doivent échanger des données avec des tiers externes à l'hôpital via Internet, la mise en œuvre d'un chiffrement des communications est obligatoire. Ce chiffrement doit reposer sur les standards et des longueurs de clés reconnus du marché. En cas de transite par un prestataire externe intermédiaire, un chiffrement des données supplémentaire au niveau applicatif est recommandé.
2.3.5 Droits d'accès		
H.TEC.16	P	**Changement des mots de passe standards** Pour les composants de l'équipement technique, raccordés au réseau de l'hôpital, les mots de passe standards (livrés avec la configuration et généralement disponibles sur Internet) – notamment des comptes administrateurs ou à forts privilèges – **doivent impérativement être changés** durant ou immédiatement après la phase d'installation.

RÉFÉRENCE	P / Q	MESURE DE SÉCURITÉ
H.TEC.17	**Q**	**Règles pour les mots de passe de comptes privilégiés** Il convient que chaque mot de passe d'un compte privilégié respecte les règles suivantes : a) Longueur minimale de 10 caractères. b) Pas de renouvellement obligatoire. c) Spécifique à l'institution. d) Interdiction d'utiliser un mot de passe contenant un élément « évident » (par exemple : l'identifiant du compte ou username, le mot de passe par défaut de l'équipement, des sigles propres à l'hôpital, au service ou au fournisseur, etc.). e) Complexité basée sur l'utilisation obligatoire d'au moins 3 des 4 catégories (majuscules, minuscules, numériques et caractères spéciaux), ou d'un générateur aléatoire. f) Conservé en lieu sûr, accessible par une liste réduite d'utilisateurs, et maintenu à jour par des responsables nommés. Ces mots de passe peuvent être gérés avec un outil spécialisé. g) Verrouillage du compte après N tentatives de login erronées (éventuellement dans un laps de temps T1). Alerte envoyée à une adresse spécifique. Déverrouillage automatique au bout d'un laps de temps T2. Par défaut : N = 5 tentatives, T1 = 1 minutes, T2 = 20 minutes. Les paramètres précis souhaités par l'hôpital (adresse pour les alertes, N, T1, T2) sont fournis sur demande. **Pour les connexions automatisées inter-systèmes** (par exemple avec un automate de monitoring ou de stockage des images), l'application de ces règles doit être décidée au cas par cas en fonction de l'impact potentiel sur la santé du patient ou l'intégrité du processus.
H.TEC.18	**P**	**Utilisation des comptes techniques** Les progiciels et applications installés sur l'équipement technique doivent s'exécuter sous une identité dotée de privilèges restreints. Le compte système « administrateur » est exclusivement réservé aux opérations de maintenance et configuration.
H.TEC.19	**Q**	**Comptes génériques** Pour les utilisateurs de l'hôpital qui doivent depuis leur poste de travail standard se connecter à l'équipement technique, l'utilisation de comptes utilisateurs **génériques** définis localement sur le système est interdite. Idéalement la gestion des comptes utilisateurs du système doit s'interfacer avec le système d'annuaire interne central de l'hôpital (Active Directory). Dans le cas contraire, le fournisseur doit fournir les procédures de gestion des comptes nominatifs adéquates, et compatibles avec les standards d'identification et d'authentification de l'hôpital (documentation à disposition sur demande).
H.TEC.20	**Q**	**Mots de passe des utilisateurs** Lors de la consultation ou du traitement des données informatiques locales de l'équipement, l'authentification des utilisateurs doit en priorité être assurée par l'annuaire central de l'hôpital (Active Directory). Lorsque cela n'est pas possible et que l'authentification est assurée par l'équipement technique, ce dernier doit s'aligner sur les règles d'identification et d'authentification de l'hôpital (documentation à disposition sur demande).
H.TEC.21	**Q**	**Modèle d'autorisation** Les droits d'accès aux données (Installation/paramétrage, données utilisateurs…) doivent être organisés et paramétrés sur la base de rôles applicatifs ou profils métiers, permettant de segmenter « qui peut accéder à quoi ». (exemple : un technicien de radiologie ne doit pas avoir accès au paramétrage du système).

RÉFÉRENCE	P / Q	MESURE DE SÉCURITÉ
H.TEC.22	**Q**	**Protection des données locales** Pour le domaine biomédical, afin de garantir la confidentialité des données médicales personnelles et nominatives qui pourraient être stockées localement sur l'équipement technique, le système doit implémenter un dispositif de chiffrement de ces données.
2.3.6 Traçabilité		
H.TEC.23	**Q**	**Journalisation (logging)** Les journaux doivent mémoriser les traces de l'ensemble des différents accès aux données. Il convient que la capacité de stockage des traces permette 6 mois de conservation minimum. Le fournisseur précisera le format et le contenu des traces. Les traces doivent contenir par exemple : date et heure, utilisateur, action prise, donnée affectée, résultat de l'opération. Les traces doivent être facilement exploitables. Par exemple, le système dispose d'une fonction d'interrogation des traces permettant notamment d'appliquer des filtres multicritères sur l'ensemble des accès et actions (par utilisateur, date, type d'accès…). Les besoins d'exportation éventuelle des traces sur media externe ne doit pas nécessiter l'interruption du fonctionnement normal du système.
2.3.7 Sauvegardes		
H.TEC.24	**Q**	**Sauvegardes des données** Les données produites par l'équipement technique qui justifient d'une durée de conservation définie par l'unité utilisatrice, doivent bénéficier d'un système de sauvegardes et de restauration. De préférence, cette sauvegarde doit reposer sur les moyens de stockage et de sauvegardes standards de l'hôpital, et en aucun cas sur de simples dispositifs locaux de type cassettes ou disques USB locaux, car ces derniers pourraient facilement être compromis voire volés. Il convient que le fournisseur estime les volumes de données stockées.
2.3.8 Maintenance		
H.TEC.25	**P**	**Accord de confidentialité (NDA)** La mise en place d'un accès de télémaintenance à l'équipement technique est soumise à l'acceptation et au retour signé de l'engagement de confidentialité de l'hôpital. ***(En ANNEXE : Accord de confidentialité, à signer)***
H.TEC.26	**P**	**Solutions de télémaintenance** Les accès de télémaintenance sur l'équipement technique doivent impérativement utiliser les services réseaux et les standards de télémaintenance proposés et approuvés par l'hôpital. La mise en place de liaisons (type modem, wifi, mobiles (3G+) ou autres) sur l'équipement technique est strictement interdite. De tels dispositifs doivent impérativement être désactivés. Les transmissions entre l'équipement technique et l'opérateur de télémaintenance sont impérativement chiffrées. En cas de transite par un prestataire externe intermédiaire, un chiffrement des données supplémentaire au niveau applicatif est recommandé. Une authentification à deux facteurs est recommandée ; sinon les adresses IP doivent être fixes.

RÉFÉRENCE	P / Q	MESURE DE SÉCURITÉ
H.TEC.27	P	**Accès de télémaintenance sortants** Les accès de télémaintenance sortants sur Internet sont restreints aux seules adresses réseau (tranche restreinte d'adresses IP) préalablement définies par le fournisseur. Ce dernier s'engage par ailleurs à communiquer par avance tout changement éventuel de ces adresses.
H.TEC.28	Q	**Autorisations en mode télémaintenance** Sauf situation d'urgence, les techniciens du fournisseur qui réalisent des opérations de maintenance ou de télémaintenance, ne sont pas autorisés à accéder à l'identité ou à des données personnelles identifiables (notamment celles des patients).
H.TEC.29	P	**Destruction des supports de données** Si une opération de maintenance requiert le remplacement d'un média (ex : disque dur) contenant des données personnelles identifiables (notamment celles des patients), le fournisseur doit impérativement remettre les supports concernés à l'hôpital (équipe Support DSI), qui en assurera la destruction selon ses procédures habituelles.
2.3.9 Conformité		
H.TEC.30	P	**Gestion des licences** Il est du ressort du fournisseur d'acquérir et de concéder à l'hôpital l'ensemble des licences d'utilisation nécessaires au fonctionnement de l'équipement concerné. Ceci concerne en particulier les droits d'usages des progiciels, des matériels et de l'ensemble des couches logiques utilisées (Système d'exploitation, algorithme, progiciels sécuritaires, progiciels réseaux, progiciels de base de données, progiciels systèmes, progiciels de transfert et de prise de main à distance, progiciels applicatifs, etc.)
H.TEC.31	P	**Droit d'audit** Le fournisseur reconnait le droit de l'hôpital d'organiser des audits de sécurité, voire de réaliser des tests d'intrusion des équipements techniques considérés.
2.3.10 Gestion des données		
H.TEC.32	Q	**Monitoring des défauts de transmission** Lorsque la remonté des données techniques ou biomédicales vers un système centralisé de l'hôpital (par exemple, le PACS pour les images) est prévue dans le cadre du projet, tout défaut de transmission doit être immédiatement signalé à l'utilisateur (par exemple via une alerte visuelle simple), ainsi qu'à l'équipe support informatique selon les outils monitoring en vigueur à la DSI (Email, Trap SNMP…)
H.TEC.33	Q	**Monitoring du stockage** Une procédure d'alerte permettant d'anticiper une éventuelle saturation des disques durs locaux (par exemple en cas de défaut de transmission) doit être prévue.

A. Annexe A (informative) – Modèle de fiche de contrôle (« checklist »)

NB : Ce modèle sert d'exemple : chaque hôpital est libre de l'adapter selon ses propres procédures.

A.1 Mode opératoire pour le fournisseur

1. Pour chaque exigence, le fournisseur doit indiquer si l'équipement est conforme (en indiquant OUI ou NON), et doit obligatoirement préciser :
    a. en cas de **conformité**, quels sont les principes retenus pour satisfaire l'exigence (pour certains points, le type de précision attendu est mentionné) ;
    b. en cas de **non-conformité**, quelles sont les raisons pour ne pas satisfaire l'exigence, et quelles mesures alternatives sont prévues ou préconisées pour maîtriser le risque.
2. Le fournisseur doit répondre à la checklist par rapport à l'équipement effectivement prévu pour implantation à l'hôpital dans le cadre du projet concerné. (S'il est jugé pertinent d'évoquer des évolutions futures, il convient de les signaler clairement comme tel.)
3. L'hôpital demande aux fournisseurs de s'engager au respect du contenu de cette checklist par la signature d'un représentant habilité.
4. En cas d'évolution technique du système impliquant un changement vis-à-vis des points de la checklist, une nouvelle version est soumise à l'hôpital pour validation.
5. La mise en place d'un équipement identique à un équipement déjà installé, ne permet pas de justifier de l'absence de fourniture de la checklist, qui reste impérative pour que le raccordement de l'équipement au réseau soit autorisé.

A.2 Identification de l'équipement technique

EQUIPEMENT TECHNIQUE	
Fabricant, marque	
Modèle, version, autres identifiants	
Type d'équipement, brève description	
Fournisseur (société, coordonnées)	

A.3 Exigences de sécurité – checklist

Exigence	P/Q	Conforme ? OUI / NON	Commentaire ou justification de non-conformité (possibilité de faire référence à des documents annexes)
H.TEC.1	**P**		
H.TEC.2	**P**		
H.TEC.3	**Q**		
H.TEC.4	**Q**		
H.TEC.5	**Q**		
H.TEC.6	**Q**		
H.TEC.7	**P**		
H.TEC.8	**P**		<Préciser la méthode et qui est responsable de l'implémentation>
H.TEC.9	**P**		<Confirmer que la mise à jour sera automatique et quotidienne>
H.TEC.10	**P**		<Préciser s'il s'agit d'un verrouillage physique ou logique du port>
H.TEC.11	**Q**		
H.TEC.12	**Q**		

H.TEC.13	P		
H.TEC.14	P		
H.TEC.15	P		<Préciser l'algorithme (AES, DES…) et la longueur des clés>
H.TEC.16	P		
H.TEC.17	Q		<Indiquer les points de conformité : a, b, c, d, e, f, g>
H.TEC.18	P		<Préciser le niveau de privilèges des comptes utilisés>
H.TEC.19	Q		<Préciser si authentification centrale (AD) ou locale>
H.TEC.20	Q		<Préciser le nombre et les types de profils>
H.TEC.21	Q		
H.TEC.22	Q		
H.TEC.23	Q		
H.TEC.24	Q		<Préciser les moyens de sauvegardes retenues>
H.TEC.25	P		
H.TEC.26	P		
H.TEC.27	P		
H.TEC.28	Q		
H.TEC.29	P		
H.TEC.30	P		
H.TEC.31	P		
H.TEC.32	Q		
H.TEC.33	Q		

A.4 Visas

	FOURNISSEUR	
Société :		Signature :
Nom et Prénom :		
Fonction :		
Lieu et Date :		

	HOPITAL	
Institution :		Remarque :
Service :		
Nom et Prénom :		
Fonction :		Signature :
Lieu et Date :		

	HOPITAL	
Institution :		Remarque :
Service :		
Nom et Prénom :		
Fonction :		Signature :
Lieu et Date :		

	HOPITAL	
Institution :		Remarque :
Service :		
Nom et Prénom :		
Fonction :		Signature :
Lieu et Date :		