DIE SPITÄLER DER SCHWEIZ
LES HÔPITAUX DE SUISSE
GLI OSPEDALI SVIZZERI

Sécurité de l'information et protection des données

Exigences concernant la sécurité informatique de systèmes tiers

Version 1.2, janvier 2020

H+: Schweizer Spitäler, Kliniken und Pflegeinstitutionen
H+: Hôpitaux, cliniques et institutions de soins suisses
H+: Gli Ospedali, le cliniche e gli istituti di cura svizzeri

Geschäftsstelle · Lorrainestrasse 4A · 3013 Bern
T 031 335 11 11 · F 031 335 11 70
geschaeftsstelle@hplus.ch · www.hplus.ch

Sommaire

1 Préambule

Outre les systèmes acquis et gérés par le service informatique interne, constitués d'une plateforme (matériel et système d'exploitation) et d'applications, l'environnement informatique d'un hôpital comprend un grand nombre de systèmes acquis de diverses manières et intégrés ou exploités en totalité ou en partie par des tiers. Ces systèmes sont désignés de manière générique par le terme de « systèmes tiers ».

Il s'agit typiquement de systèmes utilisés en technique médicale ou en technique du bâtiment. Les présentes exigences ont pour but de garantir, au moyen de mesures adéquates, la sûreté de fonctionnement des systèmes tiers afin d'assurer, de manière appropriée, la sécurité des patients, la préservation de la sphère privée des patients et des collaborateurs, la protection adéquate des systèmes tiers contre les risques informatiques, et les cyberattaques en particulier, et la non compromission d'autres systèmes du réseau hospitalier par un système tiers.

1.1 Objet et finalité

Le présent document décrit les exigences minimales en matière de sécurité informatique à respecter par les systèmes tiers pour les phases d'acquisition, d'intégration et d'exploitation. Les dispositifs médicaux sont en particulier concernés. Les exigences précisées au chapitre 2 doivent être prises en considération lors de l'acquisition de systèmes tiers dans le cadre de petits ou grands projets ou d'investissements, et lors de leur mise en service et exploitation.

Le présent document ne règle explicitement que les aspects informatiques d'un système tiers et en aucun cas ceux propres aux services métiers, qui ne sont pas déterminants d'un point de vue informatique.

1.2 Champ d'application et caractère obligatoire

Les présentes exigences ont force obligatoire pour tous les systèmes tiers, et en particulier pour tous les dispositifs médicaux, y compris leurs applications, intégrés aux infrastructures réseau locales de l'hôpital.

La base décisionnelle est constituée par l'existence d'une connexion active au réseau de l'hôpital.

Le champ d'application comprend les phases d'acquisition, d'intégration et d'exploitation. L'utilisation du catalogue d'exigences est expliquée dans l'annexe A.

Les parties concernées sont les suivantes :

- Fournisseurs (par ex. prestataire/fournisseur, intégrateur) dans le cadre de l'acquisition de systèmes tiers ;
- Collaborateurs internes qui sont, dans le cadre de l'acquisition, l'intégration ou de l'exploitation de systèmes tiers, impliqués en responsabilité, habilités à prendre des décisions ou autrement concernés, à savoir notamment les responsables des investissements et les chefs de projet.

Les annexes B à H référencées dans ce catalogue sont fournies par les institutions dans le cadre de leur processus d'acquisition de systèmes tiers. Leur contenu est propre à chaque établissement.

2 Catalogue d'exigences

2.1 Documentation

N°	Exigence	Catégorie
SEC-1.1	**Documentation de l'architecture** Le fournisseur documente l'architecture du système, respectivement de la solution globale. La documentation de l'architecture comprend au minimum : ■ Un aperçu complet de tous les systèmes, applications et composants constituant la solution ; ■ Les interfaces (sous la forme : source, cible, protocoles et but) avec les systèmes internes (hôpital) et externes existants ; ■ Autres communications de données avec des systèmes internes (hôpital) et externes (par ex. transmission de données d'utilisation, accès à distance, monitoring) existants. Le fournisseur est invité à communiquer de manière spontanée à l'hôpital, pendant toute la durée de vie du système, respectivement de la solution, les changements importants concernant la documentation de l'architecture.	☑ Obligatoire ☐ Souhaitée
SEC-1.2	**Documentation technique** Le fournisseur documente les systèmes et leur configuration sous la forme : désignation du système, système d'exploitation utilisé, applications installées avec mention du numéro de la version, services et comptes (en particulier ceux ayant des droits privilégiés), numéros de série du matériel et adresses MAC. Le fournisseur tient à jour la documentation technique pendant tout le cycle de vie du système en collaboration avec l'hôpital, ou la remet à l'hôpital pour que celui-ci le fasse. La documentation technique comprend au minimum : ■ Aperçu général de tous les systèmes constituant la solution (par ex. système d'exploitation, applications, COTS[1]/SOUP[2]) et tout autre composant important requis pour une exploitation sûre ; ■ Installation, configuration, exploitation et maintenance (sur site et/ou à distance), description de tous les systèmes, applications et composants constituant la solution, y compris leur éditeur, licence de produit et numéro de version ; ■ Matrice des ports au format suivant : source, cible, protocole réseau, port et but. La documentation technique est un élément de l'acceptation du système.	☑ Obligatoire ☐ Souhaitée
SEC-1.3	**Documentation opérationnelle** Un système est documenté par le fournisseur en collaboration avec le service métier concerné de l'hôpital. La documentation opérationnelle d'exploitation comprend au minimum: ■ Les responsabilités et contacts internes (hôpital) et externes (fournisseur), de même que les processus de maintenance, de support et d'administration concernés ; ■ La documentation pour les utilisateurs de la solution (manuel d'utilisation). Le fournisseur est invité à communiquer de manière spontanée à l'hôpital, pendant toute la durée de vie du système, les changements importants concernant la documentation opérationnelle. La documentation opérationnelle est un élément de l'acceptation du système.	☑ Obligatoire ☐ Souhaitée
SEC-1.4	**Documentation de sécurité** La documentation de sécurité comprend au minimum : ■ Politique d'entreprise en matière de sécurité et de protection des données ; ■ Certificat ISO 27'001, le cas échéant ; ■ Certificat IEC 62'304, le cas échéant ; ■ Autres certifications en matière de sécurité et de protection des données ; ■ Le document « Manufacturer Disclosure for Medical Device Security » (https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx) est disponible ; ■ Certificat CE de la solution ;	☑ Obligatoire ☐ Souhaitée

[1] COTS : Commercial off-the-shelf

[2] SOUP : Software of unknown provenance

N°	Exigence	Catégorie
	▪ Mise en œuvre des recommandations et Best Practices en matière de sécurité et de protection des données (par ex. ISO 27’018). Le fournisseur est invité à communiquer spontanément à l’hôpital, pendant toute la durée de vie du système, tous les changements importants concernant la documentation de sécurité.	
SEC-1.5	**Manufacturer Disclosure for Medical Device Security** Le document « Manufacturer Disclosure for Medical Device Security » (http://www.himss.org/resourcelibrary/MDS2) est fourni.	☑ Obligatoire ☐ Souhaitée
	Exception : le critère SEC-1.5 n’est applicable que pour les dispositifs médicaux.	
SEC-1.6	**Acceptation et mise en exploitation** Un système tiers ne peut être mis en exploitation qu’après avoir été accepté par le service métier concerné, les services de support (par ex. service technique, service biomédical) et le service informatique de l’hôpital. L’acceptation fait l’objet d’un procès-verbal écrit.	☑ Obligatoire ☐ Souhaitée

2.2 Configuration de base

N°	Exigence	Catégorie
SEC-2.1	**Plateformes et systèmes d’exploitation supportés** Le fournisseur indique si l’hôpital doit reprendre totalement ou partiellement la responsabilité de l’administration et de l’exploitation de la solution (cf. aussi SEC 1.3). Le cas échéant, la solution est basée intégralement sur les plateformes et systèmes d’exploitation supportés par l’hôpital l’annexe B.	☑ Obligatoire ☐ Souhaitée
SEC-2.2	**Système d’exploitation obsolète** L’utilisation de systèmes d’exploitation qui ne sont plus supportés par leur éditeur n’est pas autorisée. Le fournisseur indique si le système d’exploitation utilisé dans la solution proposée est pris en charge par l’éditeur, en précisant la date de « End Of Support ». Si la date « End Of Support » est située pendant la durée de vie prévue de la solution, le fournisseur indique le chemin de mise à niveau, en détaillant les éventuels coûts associés.	☑ Obligatoire ☐ Souhaitée
SEC-2.3	**Cycle de vie des produits logiciels intégrés** Le fournisseur s’engage pour tous les produits logiciels intégrés (par ex. système d’exploitation, base de données, COTS/SOUP) : ▪ A installer dans les meilleurs délais les mises à jour et mises à niveau de version publiées par les éditeurs de logiciels ; ▪ A informer immédiatement le service informatique s’il ne suit plus l’évolution des logiciels intégrés, et ce indépendamment de la durée de vie de l’appareil. Il en indique les raisons; ▪ Pour les produits Microsoft Windows, à supporter l’actuel « Current Branch for Business » (Current Branch [Semi Annual Channel] with Deferred Updates ou Long Term Servicing Channel). Pour le produit Microsoft Office, à supporter la version « On Premise » ou la version « Cloud » Office 365.	☐ Obligatoire ☑ Souhaitée
SEC-2.4	**Minimisation de l’exposition du système** Les exigences suivantes sont respectées afin de minimiser l’exposition du système : ▪ Accès Internet bloqué. Dans le cas contraire, les accès à Internet doivent être documentés ; ▪ Installation des seuls paquets logiciels et services du système d’exploitation requis ; ▪ Désinstallation ou désactivation de tous les paquets logiciels et services réseau non requis ; ▪ Installation d’un pare-feu local qui n’autorise que les accès à des ports réseau préalablement définis ; ▪ Désactivation des ports USB et autres dispositifs permettant la connexion de supports de stockage amovibles ; ▪ Désactivation des fonctions « AutoRun / AutoPlay ».	☑ Obligatoire ☐ Souhaitée

N°	Exigence	Catégorie
	Exception : hormis le point concernant l'accès à Internet, le critère SEC-2.4 n'est pas applicable pour des solutions purement applicatives. L'utilisation de l'interface USB pour des dongles à des fins de licence et d'authentification est admise ; dans ce cas, les ports USB n'ont pas à être désactivés.	
SEC-2.5	**Technologies à haut cyber risque** L'hôpital s'efforce d'éviter les technologies présentant un cyber risque élevé. Le fournisseur indique si une technologie classifiée comme étant à risque par l'hôpital fait partie de la solution. La liste des technologies à haut risque figure à l'annexe C. Le fournisseur propose le cas échéant une technologie alternative. Si aucune alternative n'est possible, les éléments suivants doivent être précisés : ■ Cas d'utilisation de la solution qui nécessitent ces technologies ; ■ Raisons pour lesquelles aucune alternative ne peut être envisagée ; ■ Plan et délai pour le remplacement de ces technologies dans la ligne de produits concernée.	☐ Obligatoire ☑ Souhaitée
SEC-2.6	**Gestion des mises à jour (Release Management)** Au moment de la livraison du système, la dernière version validée par l'éditeur doit être installée pour chaque application.	☐ Obligatoire ☑ Souhaitée
	Remarque : s'il n'est pas possible d'installer la dernière version validée, le service informatique peut isoler la solution du réseau. Il peut en tenir compte pour le calcul du TCO, ce qui a des incidences sur l'évaluation de l'offre.	
SEC-2.7	**Gestion de la sécurité (Security Management)** Le processus de gestion des mises à jour de sécurité (par ex. SecurityPatches, SecurityUpdates, SecurityFixes) repose sur les bulletins de sécurité de l'éditeur concerné. Cela concerne aussi bien le système d'exploitation que les applications. Le fournisseur communique les vulnérabilités, défauts ou dysfonctionnements de sécurité constatés dans un délai de 30 jours calendaires et s'assure que les mises à jour fournies par l'éditeur (y compris des éditeurs tiers comme Microsoft) soient installées au plus tard 60 jours calendaires après la publication du bulletin de sécurité par l'éditeur, respectivement que l'autorisation d'être installées par l'hôpital soit donnée. En cas de situation à haut risque (par ex. Wannacry), ce délai doit être raccourci selon les exigences de l'institution.	☐ Obligatoire ☑ Souhaitée
	Remarque : pour des solutions purement applicatives, le critère SEC-2.7 ne concerne que la seule application.	
	Remarque : s'il n'est pas possible d'installer la dernière version validée, le service informatique peut isoler la solution du réseau. Il peut en tenir compte pour le calcul du TCO, ce qui a des incidences sur l'évaluation de l'offre.	
SEC-2.8	**Sûreté de fonctionnement opérationnel de la solution** Le fournisseur garantit la sûreté de fonctionnement opérationnel de la solution pendant sa durée de vie au sein de l'hôpital. S'il s'avère impossible pour le fournisseur : ■ De suivre le cycle de vie des produits logiciels (cf. SEC-2.3) et/ou ■ De valider et d'installer dans les 60 jours calendaires les derniers SecurityPatches et/ou SecurityUpdates (cf. SEC-2.7), il est invité à documenter les scénarios de risque qui en résultent. Le fournisseur documente les scénarios de risque vraisemblables, en explicitant les impacts potentiels pour l'hôpital en termes de : ■ Sécurité de la prise en charge médicale ; ■ Protection des données des patients et/ou des collaborateurs ; ■ Sécurité physique des patients et/ou des collaborateurs ; ■ Conformité légale.	☐ Obligatoire ☑ Souhaitée
SEC-2.9	**Algorithme de chiffrement** Les algorithmes de chiffrement et le choix de leurs caractéristiques (par ex. longueur de la clé) répondent aux exigences des offices de référence compétents (par ex. BSI, NIST).	☑ Obligatoire ☐ Souhaitée

2.3 Protection contre les maliciels

N°	Exigence	Catégorie
SEC-3.1	**Logiciel anti-maliciels** Un logiciel anti-maliciels est installé sur tous les systèmes centraux, périphériques et clients de la solution. Un mécanisme de type « Application Whitelisting », qui bloque l'exécution de logiciels non autorisés, est également considéré comme acceptable. Des exclusions à l'activité du logiciel anti-maliciels sont possibles, et doivent être définies et documentées pour chaque système. Si le fournisseur ne propose aucun des mécanismes décrits ci-dessus, il doit justifier les raisons et préciser les scénarios de risque associés. Si l'utilisation d'un logiciel anti-maliciels entraîne la perte du marquage CE, la preuve doit en être apportée.	☑ Obligatoire ☐ Souhaitée
SEC-3.2	**Fréquence du contrôle anti-maliciels** Le logiciel anti-maliciels effectue des contrôles réguliers. Un contrôle complet est réalisé au moins une fois par semaine. Les résultats des contrôles sont mis à disposition de l'hôpital sur demande. Les maliciels détectés doivent être signalés à l'hôpital.	☑ Obligatoire ☐ Souhaitée
SEC-3.3	**Mise à jour du logiciel anti-maliciels et des signatures** Le logiciel anti-maliciels utilisé est régulièrement mis à jour, au moins une fois par jour (signatures et versions).	☑ Obligatoire ☐ Souhaitée
SEC-3.4	**Logiciel anti-maliciels standard de l'institution** Si le standard de l'hôpital est utilisé, le descriptif à l'annexe D doit être respecté. La mise à jour des signatures et versions est effectuée à partir des systèmes centraux de l'hôpital.	☐ Obligatoire ☑ Souhaitée
Exceptions : les critères SEC-3.1 à SEC-3.4 ne sont pas applicables pour les solutions purement applicatives.		

2.4 Accès au réseau

N°	Exigence	Catégorie
SEC-4.1	**Protocoles de communication sécurisés dans l'Intranet** Des protocoles de communication sécurisés (par ex. SSH, DFTP, TLS) sont utilisés pour toute communication dans l'Intranet. Toute non-conformité doit être mentionnée.	☐ Obligatoire ☑ Souhaitée
SEC-4.2	**Protocoles de communication sécurisés vers l'Internet** Des protocoles de communication sécurisés (par ex. SSH, SFTP, TLS) sont utilisés pour toute communication vers l'Internet.	☑ Obligatoire ☐ Souhaitée
SEC-4.3	**Fonctions de routage** Le système ne fournit aucune fonction de pontage (« Bridging »), de routage («Routing») ou de transfert («Forwarding») vers d'autres segments réseau. Les fonctions correspondantes doivent être désactivées.	☑ Obligatoire ☐ Souhaitée
SEC-4.4	**Adressage réseau** Le plan d'adressage réseau est prédéfini par l'hôpital ou défini en accord avec l'hôpital.	☑ Obligatoire ☐ Souhaitée
SEC-4.5	**Communications par liaison filaire** Seuls des composants du réseau de l'hôpital selon l'annexe E sont utilisés pour les communications par liaison filaire.	☑ Obligatoire ☐ Souhaitée
SEC-4.6	**Communications sans fil (WLAN)** Seuls des composants du réseau de l'hôpital selon l'annexe E sont utilisés pour les communications sans fil. Une authentification par WPA2 Enterprise / EPA-TLS est requise pour l'accès au réseau. Les certificats nécessaires à cette fin sont délivrés par l'hôpital.	☑ Obligatoire ☐ Souhaitée
SEC-4.7	**Communications sortantes vers l'Internet** Les communications sortantes vers l'Internet ne doivent être établies que vers des adresses IP définies du fournisseur de service. Un accès direct par des systèmes internes à des systèmes dans l'Internet n'est pas autorisé et doit impérativement être réalisé via la zone démilitarisée (DMZ).	☐ Obligatoire ☑ Souhaitée

N°	Exigence	Catégorie
SEC-4.8	**Authentification réseau (Network Access Control)** La solution prend en charge la méthode d'authentification réseau IEEE 802.1x. Le cas échéant, le fournisseur propose un mécanisme alternatif pour l'authentification réseau offrant un niveau de sécurité comparable.	☐ Obligatoire ☑ Souhaitée
SEC-4.9	**Synchronisation des heures systèmes** La solution prend en charge la synchronisation des heures systèmes via le protocole réseau NTP.	☑ Obligatoire ☐ Souhaitée
Exceptions: les critères SEC-4.3 à SEC-4.6 ainsi que SEC-4.8 à SEC-4.9 ne sont pas applicables pour les solutions purement applicatives.		

2.5 Réglementation des droits d'accès

N°	Exigence	Catégorie
SEC-5.1	**Règles pour les mots de passe** Les comptes d'utilisateurs locaux et génériques, en particulier les comptes d'administration et les comptes permettant l'accès à des informations sensibles, telles des données personnelles ou de patients, doivent être protégés par un mot de passe. Les règles pour les mots de passe de l'hôpital sont précisées à l'annexe F.	☑ Obligatoire ☐ Souhaitée
SEC-5.2	**Changement de mot de passe** Les mots de passe locaux et standard/par défaut doivent être modifiés avant la mise en production. Les mots de passe utilisés ne doivent pas être employés pour d'autres clients. S'il est vraisemblable que des tiers non autorisés ont pu avoir connaissance de tels mots de passe, l'hôpital doit en être informé et les mots de passe doivent être changés immédiatement.	☑ Obligatoire ☐ Souhaitée
	Remarque : le critère SEC-5.2 ne nécessite pas forcément une implémentation technique, mais peut aussi être satisfait par une mesure organisationnelle.	
SEC-5.3	**Stockage du mot de passe pour un rôle unique** Si le système n'autorise qu'un utilisateur unique par rôle, le mot de passe correspondant doit est stocké par l'hôpital.	☑ Obligatoire ☐ Souhaitée
SEC-5.4	**Blocage du compte après saisies erronées** Un compte est bloqué après trois saisies de mot de passe erronées. Un déblocage automatique est réalisé après une durée pouvant être configurée, qui doit correspondre à l'une des durées définies dans l'annexe F.	☐ Obligatoire ☑ Souhaitée
SEC-5.5	**Verrouillage de la session d'utilisateur en cas d'inactivité** Après une période d'inactivité de l'utilisateur définie à l'annexe F, la session d'utilisateur est verrouillée et une nouvelle connexion est nécessaire.	☐ Obligatoire ☑ Souhaitée
SEC-5.6	**Séparation des comptes techniques et de service** Les comptes techniques, de service et applicatif doivent être distincts. Ils doivent être dotés de droits minimaux.	☑ Obligatoire ☐ Souhaitée
SEC-5.7	**Utilisation de comptes d'administrateurs locaux** Les comptes d'administrateurs locaux ne sont utilisés que pour la maintenance et la configuration. Leur utilisation opérationnelle s'effectue avec les identifiants personnels des utilisateurs.	☑ Obligatoire ☐ Souhaitée
SEC-5.8	**Autorisation basée sur des rôles** L'autorisation est basée sur la notion de rôles. Les rôles sont au moins partiellement librement configurables.	☐ Obligatoire ☑ Souhaitée

N°	Exigence	Catégorie
SEC-5.9	**Gestion centralisée via l'Active Directory** Les solutions basées sur un système d'exploitation Windows sont intégrées dans l'annuaire Active Directory de l'institution. Les exigences suivantes sont alors automatiquement satisfaites: ■ Blocage du compte après saisies erronées (SEC-5.4) ; ■ Verrouillage de la session d'utilisateur en cas d'inactivité (SEC-5.5) ; ■ Utilisation de comptes d'administrateurs locaux (SEC-5.7).	☐ Obligatoire ☑ Souhaitée

2.6 Journalisation et traçabilité

N°	Exigence	Catégorie
SEC-6.1	**Journalisation** Toutes les opérations dans les systèmes et applications, à savoir les procédures de connexion et de déconnexion ainsi que les cas d'erreur, sont journalisées de manière à pouvoir être tracées.	☑ Obligatoire ☐ Souhaitée
SEC-6.2	**Traçabilité (Audit Trail)** La journalisation enregistre tous les accès aux données techniques, personnelles et sensibles de manière à permettre une traçabilité de qualité probante (Audit Trail).	☐ Obligatoire ☑ Souhaitée
SEC-6.3	**Protection contre la manipulation des journaux d'activités** Les journaux d'activités enregistrés temporairement ou durablement dans les systèmes doivent être protégés de toute manipulation ou accès non autorisés.	☐ Obligatoire ☑ Souhaitée
SEC-6.4	**Transmission des journaux d'activités** Les journaux d'activités peuvent être transmis à un serveur de journalisation central. Le fournisseur décrit les possibilités à cette fin (par ex. par Syslog).	☐ Obligatoire ☑ Souhaitée

2.7 Sécurité des données

N°	Exigence	Catégorie
SEC-7.1	**Traitement des données** Le fournisseur indique quelles données personnelles/sensibles et autres données nécessitant une protection appropriée sont traitées et sauvegardées par la solution : ■ Liste des données avec la justification en termes de proportionnalité et de finalité ; ■ Durée de conservation des données stockées de manière permanente ; ■ Mention des pays vers lesquels ces données pourraient être exportées.	☑ Obligatoire ☐ Souhaitée
SEC-7.2	**Stockage chiffré de données** Le stockage local de données personnelles/sensibles et autres données nécessitant une protection appropriée est effectué de manière chiffrée.	☐ Obligatoire ☑ Souhaitée
SEC-7.3	**Transmission de données** La transmission de données personnelles/sensibles et autres données nécessitant une protection appropriée à des systèmes tiers hors de l'institution n'est effectuée que si les conditions suivantes sont respectées : ■ Les données ne sont transmises que de manière chiffrée ; ■ Les données personnelles/sensibles ne sont transmises que de manière anonymisée ou pseudonymisée.	☐ Obligatoire ☑ Souhaitée
SEC-7.4	**Cycle de vie des données** Le cycle de vie des données (collecte, traitement, archivage et suppression) est documenté et tient compte des obligations de conformité internes et externes en matière de conservation.	☐ Obligatoire ☑ Souhaitée

N°	Exigence	Catégorie
SEC-7.5	**Sauvegarde et restauration des données** Le fournisseur indique, pour les données techniques, personnelles et personnelles sensibles, une estimation du volume de sauvegarde pour une durée de conservation de 10 ans. Le stockage des données générées par la solution doit être conforme aux normes applicables en Suisse et dans l'institution. La sauvegarde de ces données doit être effectuée selon les méthodes et processus standards de l'hôpital (cf. annexe G). Cette sauvegarde ne peut, en aucun cas, être faite sur un disque dur local ou un support amovible (par ex. disque dur USB).	☐ Obligatoire ☑ Souhaitée
SEC-7.6	**Destruction des données** Si des supports de stockage sont changés, les données doivent préalablement être supprimées. Le fournisseur peut également éliminer les supports de stockage de manière sûre. Il doit l'attester par écrit à l'hôpital. La destruction physique des supports de données est conforme à la norme DIN 66399 (classe de protection 2). La suppression sûre des données est effectuée selon le standard VSIT de l'office fédéral allemand de la sécurité de l'information (BSI) ou le standard DoD-5220.22-M (E).	☑ Obligatoire ☐ Souhaitée

2.8 Maintenance et assistance

N°	Exigence	Catégorie
SEC-8.1	**Processus standard d'accès à distance** L'accès à distance est effectué en utilisant le standard de l'hôpital conformément à l'annexe H. Toute autre possibilité de connexion doit être désactivée. Si le standard de l'hôpital ne peut être mis en œuvre pour la solution, le fournisseur doit en donner les raisons et proposer un mécanisme alternatif présentant un niveau de sécurité comparable.	☐ Obligatoire ☑ Souhaitée
SEC-8.2	**Accès à distance** Un accès à distance à des systèmes de l'institution est effectué sans exception en respectant les exigences suivantes : ■ Les accès sont chiffrés; ■ Les accès sont enregistrés de manière non altérables. Il s'agit de pouvoir retracer quelle personne (qui) a accédé à quel système (quoi ?), à quelle heure (quand ?) ; ■ Les accès sont authentifiés au moins une fois au moyen d'un identifiant personnel de l'utilisateur, de préférence sur les systèmes de l'institution. Si cette authentification n'est pas effectuée sur les systèmes de l'institution, les journaux d'activités sont fournis régulièrement ou sur demande par le fournisseur à l'hôpital, sans assistance de la part de ce dernier.	☑ Obligatoire ☐ Souhaitée
SEC-8.3	**Annonce de travaux de maintenance** Tous les travaux de maintenance réalisés par le fournisseur, qu'il s'agisse de travaux sur site ou à distance, doivent préalablement être annoncés aux services métier et de support. Si des circonstances particulières nécessitent des travaux de maintenance immédiats, ceux-ci seront signalés aux services métier et de support dans les 24 heures, avec une justification compréhensible de l'urgence.	☑ Obligatoire ☐ Souhaitée

2.9 Intégration

N°	Exigence	Catégorie
SEC-9.1	**Surveillance des erreurs de transmission** Le fournisseur indique si une transmission de données de la solution à un système centralisé de l'hôpital (par ex. PACS) est prévue, et si et sous quelle forme, une erreur de transmission est immédiatement signalée à l'utilisateur et au service informatique. Comment peut-on détecter, par ex., qu'un système d'imagerie ne fournit plus ses données à l'archive d'images (protection contre la perte de données)?	☐Obligatoire ☐Souhaitée

N°	Exigence	Catégorie
SEC-9.2	**Modèle d'intégration des données** Le fournisseur indique si la solution supporte un modèle d'intégration reposant sur le concept de « Web Service ». Le cas échéant, il joint la documentation technique des « Web Services » proposés par la solution. Si ce mode d'intégration n'est pas supporté, le fournisseur précise comment sa solution peut être intégrée à une architecture SOA (par ex. à l'aide d'un proxy). Si aucune alternative n'est envisageable, le fournisseur précise si le support de « Web Services » figure sur la feuille de route de la solution et dans quel délai ceux-ci seront disponibles.	☐Obligatoire ☐Souhaitée

2.10 Conformité

N°	Exigence	Catégorie
SEC-10.1	**Accord contractuel** L'utilisation de systèmes (par ex. système d'exploitation) et d'applications qui ne sont plus supportés n'est pas autorisée. Cela inclut des applications ou composants d'éditeurs tiers requis pour l'exploitation de la solution. L'accord contractuel entre l'hôpital et le fournisseur précise que ce dernier respecte le cycle de vie indiqué par les éditeurs des systèmes et applications utilisés. Le fournisseur informe l'hôpital dès que le développement des applications utilisées est interrompu.	☑ Obligatoire ☐ Souhaitée
SEC-10.2	**Accord de confidentialité (NDA)** Un accord de confidentialité conforme au droit suisse est négocié ou remis comme élément de l'accord contractuel. Le modèle proposé par l'hôpital est privilégié.	☑ Obligatoire ☐ Souhaitée
SEC-10.3	**Déclaration des flux de données** Si des données sont transmises à des tiers (par ex. données pour le dépannage ou le contrôle qualité), celles-ci doivent être explicitées dans le détail sous la forme : but, contenu des données, protection de la confidentialité en cas de transmission et de stockage.	☑ Obligatoire ☐ Souhaitée
SEC-10.4	**Stockage des données** Les données personnelles/sensibles et autres données nécessitant une protection appropriée sont exclusivement stockées en Suisse ou dans un pays offrant un niveau de protection des données approprié. La liste des pays publiée par le préposé fédéral à la protection des données et à la transparence (PFPDT), dans sa version en vigueur, est applicable. La date de référence est la date de l'offre. En cas d'hébergement de données hors de Suisse, une offre de stockage en Suisse est souhaitée comme option. La décision définitive sur le lieu de stockage des données est prise par l'hôpital pendant la phase d'évaluation.	☑ Obligatoire ☐ Souhaitée
SEC-10.5	**Accès à distance** L'accès à distance est réalisé intégralement depuis la Suisse ou un pays offrant un niveau de protection des données approprié. La liste des pays publiée par le préposé fédéral à la protection des données et à la transparence (PFPDT), dans sa version en vigueur, est applicable. La date de référence est la date de l'offre.	☑ Obligatoire ☐ Souhaitée
SEC-10.6	**Couverture en licence** Le fournisseur est responsable de la couverture réglementaire en licence pour les composants qu'il a livrés. Le fournisseur garantit des droits d'utilisation illimités et s'assure que tous les composants soient mis à jour en fonction des besoins. Le cas échéant, le fournisseur s'engage à signer un contrat Escrow.	☑ Obligatoire ☐ Souhaitée
SEC-10.7	**Test d'intrusion** Le fournisseur reconnaît le droit à l'hôpital de réaliser des vérifications de sécurité nécessaires (par ex. audit de sécurité, test d'intrusion) de sa propre autorité et garantit à l'institution, respectivement au mandataire de l'hôpital, un accès sans restrictions aux documents nécessaires.	☑ Obligatoire ☐ Souhaitée
SEC-10.8	**Exploitation autonome du réseau** Les systèmes autonomes peuvent être exploités (sous charge) de manière indépendante pendant au moins huit heures.	☐ Obligatoire ☑ Souhaitée

Annexe A Utilisation du catalogue d'exigences

Le prestataire doit prendre position sur toutes les exigences du catalogue du chapitre 2 en remplissant la fiche de contrôle de manière auto déclarative.

A.1 Phase

- **Acquisition**
  Les exigences précisées au chapitre 2 doivent être prises en compte par le fournisseur pour l'acquisition d'un système.
- **Intégration**
  Les exigences précisées au chapitre 2 doivent être prises en compte par le fournisseur pour l'intégration d'un système.
- **Exploitation**
  Les exigences précisées au chapitre 2 doivent être prises en compte par le fournisseur pour l'exploitation d'un système.

A.2 Catégorie

- **Obligatoire**

  Les exigences obligatoires doivent impérativement être satisfaites. Le non-respect d'une ou de plusieurs exigences obligatoires lors de l'acquisition entraîne l'exclusion de l'offre. Outre une satisfaction directe d'une exigence obligatoire, une réalisation indirecte est aussi autorisée. Par satisfaction indirecte, il faut comprendre une satisfaction de l'exigence en tenant compte de mesures et dispositions supplémentaires. Ces mesures et dispositions supplémentaires doivent être expliquées dans une annexe.

- **Souhaité**

  Les exigences souhaitées servent, de manière cumulée, à la qualification du système pris en compte lors de l'appel d'offres.

A.3 Conformité

- **Oui**

  L'exigence est satisfaite.

- **Non**

  L'exigence n'est pas réalisée.

- **Non applicable**

  L'exigence n'est pas applicable. Ce niveau de satisfaction n'est autorisé que pour les exigences pour lesquelles des exceptions sont définies dans le catalogue et dans la mesure où les conditions qui y sont décrites sont remplies. Le niveau de satisfaction est dans tous les cas décrit de manière détaillée et compréhensible.