Exigences de sécurité de base pour les systèmes informatiques

Sécurité de l'information et protection des données

Version 2.7 de mai 2025

Table des matières

1 Introduction

1.1 Objet et but

Outre les systèmes fournis et gérés à l'interne par le service informatique, à savoir la plateforme (matériel et système d'exploitation) et les applications, l'environnement système d'un établissement de santé comprend une multitude de systèmes acquis ailleurs et intégrés complétement ou partiellement par des tiers.

La présente directive définit les exigences minimales techniques et organisationnelles en matière de sécurité de l'information et de protection des données applicables aux systèmes de l'établissement de santé. L'objectif de ce document est de garantir la sécurité d'exploitation des systèmes et, par conséquent, la sécurité des patient·e·s, la protection de la sphère privée des patient·e·s et du personnel, ainsi que la protection adéquate des systèmes contre les cybermenaces.

Afin de garantir une large acceptation de ces exigences, la coordination avec les principaux acteurs du marché est essentielle. Le H-CSC harmonise donc ces exigences de sécurité de base avec l'association des hôpitaux H+ et le réseau pour la technique hospitalière IHS « Infrastructure Hôpital Suisse ».

Les principaux fournisseurs sont également impliqués afin que les exigences soient compréhensibles et transparentes pour eux et que les processus d'approvisionnement communs puissent être soutenus de manière optimale.

1.2 Délimitation

La présente directive définit les exigences de sécurité de base en matière de sécurité de l'information et de protection des données. Elle ne traite pas d'autres exigences telles que les heures de service, la convivialité ou les exigences techniques des systèmes.

L'externalisation de l'exploitation des systèmes à un prestataire de services entraîne des exigences supplémentaires, qui ne font pas partie intégrante de la présente directive. Cela vaut également pour l'utilisation de logiciels en tant que services (SaaS).

1.3 Champ d'application

La présente directive s'applique à tous les systèmes, en particulier à tous les systèmes médicaux et leurs applications, qui sont intégrés dans l'infrastructure réseau locale de l'établissement de santé et/ou qui traitent des données de l'établissement de santé (données de patient·e·s, données du personnel ainsi que données commerciales de nature médicale ou non).

Elle s'applique également aux systèmes médicaux pouvant être mis en réseau, même s'ils ne sont pas connectés au réseau informatique de l'établissement de santé (cf. art. 74 ODim[1]).

Le document couvre les phases d'acquisition, de mise en service, d'exploitation et de mise hors service.

Sont principalement concernés les groupes suivants :

- les prestataires de services et les fournisseurs ;
- le personnel interne des établissements de santé qui, dans le cadre de l'acquisition, de l'intégration, de l'exploitation et de la mise hors service des systèmes, sont responsables, habilités à prendre des décisions ou impliqués d'une autre manière, notamment les responsables des investissements et de projets.

  Remarque : Pour les établissements de santé membres du H-CSC, d'autres documents sont disponibles sur la plateforme H-CSC afin de soutenir la mise en œuvre interne de ces directives. Il s'agit notamment de présentations destinées à convaincre la direction ou les services d'achat, d'un guide pour l'application des exigences de sécurité de base pour les systèmes informatiques dans le processus d'acquisition ou dans les appels d'offres publics (soumissions).

1.4 Bases

La présente directive se fonde sur les lois et prescriptions émises par les autorités de réglementation nationales et cantonales ainsi que sur les normes techniques et organisationnelles reconnues.

1.5 Caractère contraignant et marge de manœuvre

Les présentes exigences de sécurité de base pour les systèmes informatiques deviennent contraignantes lorsqu'elles sont exigées par l'établissement de santé concernée vis-à-vis des fournisseurs (p. ex. dans le cadre de demandes d'offres, de documents d'appel d'offres, de conditions d'achat, etc.).

Les exigences de sécurité de base évoluent en fonction de l'état de la technique, mais doivent rester aussi stables que possible tant pour les établissements de santé que pour les fournisseurs. Ni les établissements de santé ni les fournisseurs ne devraient être confrontés à des exigences formulées différemment et structurées de manière variable pour les mêmes systèmes.

Néanmoins, les exigences doivent pouvoir être adaptées aux capacités d'un établissement de santé ou à une acquisition spécifique d'un système. Pour cette raison, deux modes d'application différents de ces exigences sont prévus.

Spécification : pour les processus d'acquisition réactifs des établissements de santé

Les institutions de santé peuvent renforcer ou assouplir certaines exigences de sécurité de base dans leur ensemble. Ces écarts ainsi que la pondération des exigences sont définis par l'établissement de santé dans un document séparé intitulé *Exigences de sécurité de base pour les systèmes informatiques – **Spécification*** et transmis directement aux fournisseurs. Grâce à la spécification, les écarts sont facilement identifiables pour les fournisseurs. Le contenu des exigences n'est toutefois pas modifié (baseline).

[1] Ordonnance du 1er juillet 2020 sur les dispositifs médicaux ; RS *812.213*

Autodéclaration : pour les processus d'approvisionnement proactifs des fournisseurs

L'autodéclaration permet à un fournisseur de vérifier et de documenter une seule fois ses produits par rapport aux exigences de sécurité de base. Cette autodéclaration peut ensuite être utilisée par le fournisseur dans ses processus d'approvisionnement proactifs pour tous les établissements de santé. Un modèle correspondant est mis à disposition sur le site web du H-CSC.

1.6 Définitions des concepts

Terme	Définition
Établissement de santé	Organisation dont l'objectif principal est de prendre en charge ou traiter des patientes et patients ou encore de promouvoir la santé publique. Cela comprend notamment les hôpitaux, les cliniques et les établissements de soins.
Système	Matériel ou logiciel fourni, intégré et/ou exploité en totalité ou en partie par un tiers. Le système comprend tous les composants fournis par un fournisseur ou un prestataire de services. Cela inclut le matériel, les micrologiciels, les systèmes d'exploitation, les pilotes, les intergiciels, les applications auxiliaires et principales, ainsi que tous les composants que le fournisseur ou le prestataire de services utilise et qui proviennent de sous-traitants. Par exemple, des modules d'extension (*add-ons / plug-ins*), des codes sources intégrés ou des bibliothèques de liens.
Appareil mobile	Appareil qui, en raison de sa taille et de son poids, peut être transporté sans effort physique important, utilisé de manière mobile et/ou soustrait à la zone de responsabilité de l'établissement de santé sans que l'on s'en aperçoive. Exemples : ordinateurs portables, tablettes, smartphones ou petits appareils médicaux. Un appareil mobile peut faire partie d'un système.
Traitement de données	Toute opération effectuée sur des données, telle que la collecte, la conservation, l'enregistrement, l'utilisation, la consultation, la modification, la publication ou la destruction de données.

1.7 Structure du document

Afin d'aider les fournisseurs de dispositifs médicaux, il convient de fournir des références à la *Manufacturer Disclosure Statement for Medical Device Security* [R02] lorsque c'est utile.

Toutes les exigences et clauses contractuelles types sont accompagnées d'une référence (ID) unique dans la présente directive.

2 Exigences

2.1 Principes

ID	Exigence
01.01	Conception de la sécurité : Il faut garantir à tout moment et dans tous les domaines que le fonctionnement du système ne cause aucun préjudice aux personnes ni à l'établissement de santé. Les vulnérabilités sont prises au sérieux et corrigées rapidement.
01.02	Connaissance du système et compatibilité : Le fournisseur doit connaître tous les composants qui constituent le système. Il doit s'assurer que ces composants sont compatibles entre eux à tout moment au sein du système.
01.03	Defense-in-depth : Un système doit être protégé par différentes mesures de sécurité se complétant entre elles afin d'assurer la redondance de la sécurité. Les mesures de sécurité visent un effet global de prévention, de détection et de réaction.

ID	Exigence
01.04	Least privilege et need-to-know : L'octroi de droits d'accès et de privilèges doit être limité au minimum. Cela vaut pour les utilisateurs d'un système, les services et les fonctionnalités supplémentaires activés ainsi que les relations de communication autorisées.
01.05	Security by default : Les systèmes doivent être développés, configurés et exploités de telle sorte que toutes les mesures de sécurité pertinentes dans un environnement spécifique soient activées par défaut et puissent déployer leurs effets sans que les utilisateurs aient à s'en soucier. Les composants du système qui gèrent les autorisations d'accès doivent être conçus de sorte qu'aucun accès non autorisé ne soit possible en cas de dysfonctionnement.
01.06	Privacy by design et privacy by default : Les mesures de protection des données sont intégrées de manière systématique dans les processus de développement des systèmes. Les systèmes sont développés de sorte que des paramètres de protection des données sûrs soient définis comme standard dès le départ.

2.2 Organisation

ID	Exigence
02.01	Responsabilités : Les tâches, compétences et responsabilités relatives au système sont convenues entre l'établissement de santé et le fournisseur avant la conclusion du contrat. Les responsabilités relatives aux différents composants d'un système ainsi que celles relatives au bon fonctionnement d'un système utilisant aussi des composants fournis par l'établissement de santé sont notamment définies.
02.02	Responsabilité du système : Le fournisseur est responsable du bon fonctionnement de tous les composants du système compris dans la livraison. Cela inclut également l'interaction avec les composants fournis par l'établissement de santé et conformes aux spécifications convenues par écrit.
02.03	Obligation d'annoncer les incidents de sécurité : Les incidents de sécurité (cyberattaques ; y c. violations de la protection des données) survenus chez les fournisseurs et leurs sous-traitants sont signalés dans les délais légaux (loi sur la sécurité de l'information). Le service compétent au sein de l'établissement de santé doit être informé dans les 24 heures suivant la détection, puis tenu activement informé [R03].
02.04	Gestion active du cycle de vie : Le fournisseur s'assure de respecter les cycles de vie prescrits par les fabricants pour tous les composants (y c. les applications, les systèmes d'exploitation, etc.) des systèmes fournis. Les composants pour lesquels plus aucune mise à jour de sécurité n'est disponible doivent être remplacés. Réf. MDS2 : DOC-8
02.05	Gestion active des vulnérabilités : Le fournisseur assure la gestion des vulnérabilités (*vulnerability management*) pour tous les composants du système. Il vérifie régulièrement les composants du système afin de détecter les vulnérabilités et suit les notifications de vulnérabilité émises par les fabricants des composants. Le fournisseur informe l'établissement de santé de manière active et transparente des nouvelles vulnérabilités dès qu'il les découvre, indépendamment du fait qu'une contremesure soit déjà disponible. Le service informatique de l'établissement de santé indique au fournisseur un interlocuteur pour ces annonces [R03]. Réf. MDS2 : CSUP-11 Réf. MDS2 : RDMP-4
02.06	Interlocuteur pour les annonces de vulnérabilité : Au sein de son entreprise, le fournisseur désigne un interlocuteur auquel l'établissement de santé peut annoncer les vulnérabilités

ID	Exigence
	identifiées. Il veille à ce que ces annonces soient traitées rapidement par des spécialistes de son entreprise et à ce que l'établissement de santé soit informé des résultats.
02.07	Correction des vulnérabilités : Le fournisseur met à disposition tous les moyens nécessaires pour corriger les vulnérabilités. Les correctifs de sécurité sont installés rapidement à partir du moment où ils sont disponibles, en fonction du niveau de gravité de la vulnérabilité dans le classement le plus récent du *Common Vulnerability Scoring System* (CVSS), ou ils sont validés pour installation sur les systèmes de l'établissement de santé.
02.08	Délais pour la correction de vulnérabilités : Les délais impartis pour corriger les vulnérabilités sont basés sur le CVSS. Les niveaux de gravité des vulnérabilités sont : ▪ Critique (CVSS = 9.0 – 10.0) : aussi vite que possible[1] ▪ Élevé (CVSS = 7.0 – 8.9) : 2 semaines ▪ Moyen (CVSS = 4.0 – 6.9) : 1 mois ▪ Faible (CVSS = 0.1 – 3.9) : 2 mois [1] Le temps dépend des risques qu'une application ne soit pas disponible. Si des composants du système sont fournis par l'établissement de santé en vertu d'un accord passé avec le fournisseur, l'établissement de santé est responsable de leur mise à jour. La responsabilité globale du bon fonctionnement du système incombe au fournisseur. Ce dernier indique à l'établissement de santé les composants à utiliser pour la mise à jour et s'assure de leur compatibilité avec l'ensemble du système.
02.09	Autorisation de mise en service : Le système n'est mis en service qu'après réception par les services concernés (par ex. technique du bâtiment, informatique médicale et technologie médicale) et le service informatique de l'établissement de santé [R03]. La réception fait l'objet d'un procès-verbal écrit.
02.10	Transfert de propriété de systèmes physiques : Les systèmes et tous leurs composants ne peuvent quitter l'établissement de santé qu'avec l'autorisation du personnel informatique compétent [R03]. Avant le transfert de propriété de systèmes ou de composants, quelle qu'en soit la raison, les données de l'établissement de santé doivent être irréversiblement effacées [05.05] ou détruites de manière sécurisée [05.06]. Une déclaration écrite ad hoc doit être remise au personnel informatique compétent avant le transfert de propriété.

2.3 Documentation

ID	Exigence
03.01	Documentation relative à l'architecture : L'architecture du système ou de la solution globale est entièrement documentée. La documentation relative à l'architecture comprend au minimum les points suivants : 1. vue d'ensemble complète sous forme graphique de tous les systèmes, applications et composants associés à la solution ; 2. certificats de tous les composants des produits logiciels utilisés et de leurs relations au sein de la chaîne logistique logicielle (nomenclature produits logiciels) ; 3. interfaces avec les systèmes internes et externes existants, avec au moins les informations suivantes : source, destination, protocole(s), chiffrement, authentification, objets de données transférés avec classification de confidentialité et indication de la finalité ;

ID	Exigence
	4. communications de données vers des systèmes internes et externes existants (par ex. transmission de données de consommation, accès à distance, surveillance) ; 5. flux de données sous la forme suivante : finalité, contenu des données, protection de la confidentialité pendant le transfert et le stockage des données. La classification des niveaux de confidentialité des objets de données est régie par les directives ad hoc de l'établissement de santé [R03]. Réf. MDS2 : DOC-10
03.02	Documentation technique d'exploitation : Une documentation technique d'exploitation est fournie avec le système. Elle comprend au moins les points suivants : 1. vue d'ensemble complète de tous les systèmes liés à la solution (par ex. système d'exploitation, applications, COTS[2]/SOUP[3]) et de tous les autres composants essentiels pour un fonctionnement stable et sûr ; 2. installation, configuration, exploitation et maintenance (sur site et/ou à distance), description de tous les systèmes, applications et composants liés à la solution, y compris leur éditeur, licence produit et numéro de version ; 3. systèmes et leur configuration sous la forme suivante : désignation du système, système d'exploitation utilisé, applications installées avec indication des numéros de version, services et comptes (en particulier ceux disposant d'autorisations privilégiées) ; 4. liste de tous les supports électroniques du système sur lesquels des données de l'établissement de santé pourraient être enregistrées ; indiquer le type de support (par ex. SSD, disque dur) et l'emplacement physique dans l'appareil afin de pouvoir retrouver les supports ; 5. déclaration de tous les emplacements de stockage temporaire et permanent des données, avec indication des données de l'établissement de santé qui y sont enregistrées ; 6. marquage des points de contrôle à surveiller pour garantir un fonctionnement irréprochable, avec les paramètres nécessaires pour le garantir ; 7. matrice de communication sous la forme suivante : source, destination, protocole réseau, port et finalité. Réf. MDS2 : DOC-10 Réf. MDS2 : SBOM-1
03.03	Documentation opérationnelle : Une documentation opérationnelle est établie pour le système et coordonnée avec le service compétent de l'établissement de santé [R03]. Cette documentation comprend au moins : 1. les responsabilités et les contacts internes (établissement de santé) et externes (fournisseurs) ainsi que les processus de maintenance, d'assistance et d'administration associés, en particulier : a) la déclaration de responsabilité opérationnelle des composants du système, b) les instructions pour le support de premier niveau sur la manière de procéder en cas d'erreurs connues, c) les instructions pour le support de deuxième niveau sur la manière d'analyser les erreurs et quand les transmettre au support de troisième niveau (fabricant), d) les instructions pour arrêter correctement les composants du système et e) les instructions pour démarrer correctement les composants du système ;

[2] Commercial of the shelf software
[3] Software of unknown pedigree

ID	Exigence
	2. la documentation utilisateur de la solution (manuel d'utilisation).
03.04	Documentation de sécurité : Le fournisseur fournit la documentation de sécurité suivante concernant le produit proposé et sa propre organisation : 1. *Information Security Policy* ; 2. certificat ISO 27001, le cas échéant ; 3. application des recommandations et des bonnes pratiques en matière de sécurité et de protection des données (par ex. ISO 27018) ; 4. autres certifications dans le domaine de la sécurité et de la protection des données, le cas échéant ; 5. instructions pour démarrer un système après un échec et vérifier l'intégrité des données ; 6. instructions pour rétablir le fonctionnement normal après un fonctionnement restreint (mode sans échec). Réf. MDS2 : SGUD-1
03.05	Documentation de sécurité pour les systèmes médico-techniques : Les systèmes médico-techniques disposent des certifications suivantes : 1. certificat IEC 62304 ; 2. certificat CE ; 3. *Manufacturer Disclosure Statement for Medical Device Security* (MDS2). Réf. MDS2 : RDMP-1
03.06	Documentation pour la réception : Lors de la réception du système par l'établissement de santé, la documentation suivante doit être disponible : ▪ documentation relative à l'architecture ; ▪ documentation technique d'exploitation ; ▪ documentation opérationnelle ; ▪ documentation de sécurité. Le cas échéant, documentation de sécurité relative aux systèmes médico-techniques.
03.07	Forme de la documentation : La documentation est fournie sous forme électronique dans un format courant (par ex. PDF).
03.08	Contrôle : Toute la documentation doit être soumise à l'approbation de l'établissement de santé. La mise en service du système n'aura lieu qu'après validation de la documentation. Toutes les modifications apportées à la documentation, à l'exception des modifications mineures, sont activement portées à la connaissance de l'établissement de santé pendant toute la phase d'exploitation du système et, si nécessaire, convenues à l'avance.

2.4 Configuration de base

ID	Exigence
04.01	Réduction de l'exposition du système : Les mesures suivantes sont mises en œuvre afin de minimiser l'exposition du système : 1. blocage de l'accès à Internet dans la mesure où celui-ci n'est pas nécessaire au fonctionnement des composants ou à l'exploitation ; 2. désinstallation ou désactivation de tous les paquets logiciels et services réseau non nécessaires. Seuls les paquets logiciels et services absolument indispensables au

ID	Exigence
	fonctionnement du système doivent être installés. Si des composants auxiliaires sont installés temporairement (par ex. pendant une maintenance), ils doivent être désinstallés une fois les travaux terminés ; 3. installation d'un pare-feu local autorisant uniquement l'accès à des ports réseau prédéfinis ; 4. désactivation, entre autres, des ports USB et des interfaces Bluetooth, ainsi que des autres possibilités de connexion, dans la mesure où celles-ci ne sont pas utilisées dans le cadre de l'exploitation ; 5. désactivation des fonctions d'exécution et de lecture automatiques (*autorun / autoplay*). Réf. MDS2 : SAHD-1
04.02	Utilisation de technologies à risque : Il est interdit d'utiliser des technologies présentant des risques connus pour la sécurité, telles que les protocoles SMBv1, FTP ou Telnet. Réf. MDS2 : TXCF-5
04.03	Restriction des interfaces : Les communications sont établies exclusivement via les interfaces convenues et documentées avec l'établissement de santé. Les interfaces non utilisées sont désactivées afin qu'aucune communication ne soit possible via celles-ci.
04.04	Endpoint protection : Le système doit être protégé contre les logiciels malveillants et l'utilisation abusive des composants du système à l'aide d'une solution de protection des terminaux (*endpoint protection*). Si l'utilisation d'une solution de ce type compromet la conformité (CE, MDR, etc.) du système, le fournisseur en informe le client. Réf. MDS2 : MLDP-2
04.05	Mise à jour de la endpoint protection : Les mises à jour de sécurité pour la solution Endpoint Protection sont installées régulièrement, au moins une fois par jour, et les nouvelles versions sont installées dans les meilleurs délais. Le système peut se connecter à internet pour effectuer les mises à jour de sécurité [04.01].

2.5 Sécurité des données

ID	Exigence
05.01	Stockage des données chiffré : Les données sont traitées conformément aux prescriptions de classification de l'établissement de santé [R03]. Les données sensibles et les données personnelles sont chiffrées au minimum « *at rest* » à l'aide d'un procédé cryptographique sécurisé ; cela vaut en particulier pour la conservation des données sur des appareils mobiles. Réf. MDS2 : STCF-1
05.02	Procédés cryptographiques sécurisés : Seuls des procédés cryptographiques et des longueurs de clé considérés comme sûrs sont utilisés pour le chiffrement des données. L'établissement de santé se conforme à cet égard à la directive technique TR-02102 de l'Office fédéral allemand pour la sécurité informatique (BSI) [R01].
05.03	Transmission et stockage des données : Le fournisseur n'enregistre aucune donnée de l'établissement de santé sur son infrastructure informatique ou ses supports de stockage (clés USB, disques, etc.), ni ne les transmet à quiconque. Sont exclues de cette exigence les données système qui sont absolument nécessaires pour garantir le fonctionnement. Les données ne sont pas supprimées des systèmes de l'établissement de santé sans le consentement écrit des responsables de l'établissement [R03].

ID	Exigence
	Si des systèmes d'informatique en nuage (*cloud*) sont utilisés pour traiter ou stocker des données, ceux-ci doivent être documentés et leur utilisation doit être explicitement autorisée par l'établissement de santé.
05.04	Cycle de vie des données : Le cycle de vie des données (collecte, traitement, archivage et suppression) est documenté et tient compte des exigences de conformité (*compliance*) internes et externes relatives à l'obligation de conservation des données incombant aux établissements de santé [R03]. Le système ne supprime les données de lui-même que si cette suppression est autorisée par les lois et les directives internes applicables à l'établissement de santé. Le système fournit une interface permettant de transférer les données pertinentes pour l'établissement de santé vers le système d'archivage conformément à la législation (par ex. les données relatives aux soins). La sauvegarde des données s'effectue selon les méthodes et processus standard de l'établissement de santé [R03].
05.05	Suppression sécurisée : Le système prend en charge des fonctions de suppression sécurisée qui peuvent être utilisées pour supprimer de manière irréversible toutes les données de l'établissement de santé stockées sur des supports de données locaux. Il s'agit notamment de toutes les données relatives aux patients, des données d'accès telles que les mots de passe et les clés, des statistiques d'utilisation, des résultats de mesures, etc. Ces fonctions de suppression doivent être conformes à la norme VSIT de l'Office fédéral allemand pour la sécurité (BSI) ou à la norme DoD-5220.22-M (Département de la Défense américain) et décrites en détail par le fournisseur dans la documentation. Après la suppression, seules les informations correspondant à la configuration initiale du système et à l'état d'usine doivent se trouver sur l'appareil.
05.06	Destruction des données : Lors du remplacement des supports de stockage, toutes les données qui y sont enregistrées doivent être préalablement effacées de manière sécurisée [05.05]. Le fournisseur peut également détruire les supports de données de manière sécurisée et les éliminer dans le respect de l'environnement ou les remettre à l'établissement de santé pour destruction. Il en informe l'établissement de santé par écrit. Les supports de données ne doivent pas quitter l'établissement de santé sans l'accord écrit des responsables. La destruction physique des supports de données est effectuée conformément à la norme DIN 66399, classe de protection 2 [R04]. Réf. MDS2 : SGUD-2

2.6 Protection des données

ID	Exigence
06.01	Gestion centralisée : L'accès aux données personnelles sensibles sur les systèmes de l'établissement de santé s'effectue exclusivement via des comptes utilisateurs personnels, qui sont gérés de manière centralisée par l'établissement de santé. Il n'y a pas d'accès aux données pour les utilisateurs locaux. Réf. MDS2 : AUTH-1.1
06.02	Traitement des données : Le traitement des données personnelles et autres données sensibles est effectué exclusivement en Suisse ou dans un pays offrant un niveau de protection adéquat. La loi applicable à l'établissement de santé concerné (droit national ou cantonal)

ID	Exigence
	est celle en vigueur, dans sa version la plus récente. La date de référence est la date de l'offre ou de l'achat.
06.03	Liste des données personnelles : Le fournisseur indique quelles données à caractère personnel sont traitées et enregistrées par le système : 1. présentation des données avec justification de la proportionnalité et de la finalité ; 2. durée de conservation des données stockées à long terme ; 3. mention des pays vers lesquels ces données sont susceptibles d'être exportées (stockage, sauvegarde, accès). Réf. MDS2 : MPII-1 Réf. MDS2 : MPII-2 Réf. MDS2 : MPII-3

2.7 Journalisation et traçabilité

ID	Exigence
07.01	Enregistrement : Toutes les actions portant sur le système, dont : ▪ les procédures de connexion et de déconnexion, ▪ les dysfonctionnements, ▪ l'exécution de fonctions privilégiées et de fonctions d'administrateur, ▪ la modification des droits d'accès et des rôles des utilisateurs et ▪ la modification de la configuration des systèmes, sont enregistrées dans un journal selon les principes de la traçabilité. Réf. MDS2 : AUDT-1 Réf. MDS2 : AUDT-1.1 Réf. MDS2 : AUDT-1.2 Réf. MDS2 : AUDT-2.1 Réf. MDS2 : AUDT-2.2
07.02	Audit-trail : Le journal répertorie tout traitement de données techniques, personnelles ou particulièrement sensibles selon une piste d'audit (*audit trail*). Réf. MDS2 : AUDT-2 Réf. MDS2 : AUDT-2.1 Réf. MDS2 : AUDT-2.2 Réf. MDS2 : AUDT-2.3 Réf. MDS2 : AUDT-2.4 Réf. MDS2 : AUDT-2.5 Réf. MDS2 : AUDT-2.6 Réf. MDS2 : AUDT-2.7 Réf. MDS2 : AUDT-2.8 Réf. MDS2 : AUDT-2.8.1 Réf. MDS2 : AUDT-2.8.2 Réf. MDS2 : AUDT-2.9 Réf. MDS2 : AUDT-2.10 Réf. MDS2 : AUDT-2.11
07.03	Protection contre la manipulation des données du journal : Les données de journal enregistrées temporairement ou à long terme sur le système sont protégées contre toute manipulation et tout accès non autorisé. Réf. MDS2 : AUDT-7
07.04	Transmission des données du journal : Le système est capable de transmettre les données du journal à un serveur centralisé de l'établissement de santé via une interface et un format standardisés (par ex. Syslog).

ID	Exigence
	Réf. MDS2 : AUDT-5 Réf. MDS2 : AUDT-5.1 Réf. MDS2 : AUDT-5.2 Réf. MDS2 : AUDT-5.3

2.8 Communication et accès réseau

ID	Exigence
08.01	Protocoles de communication sécurisés : Le système utilise exclusivement des protocoles de communication avec des procédés cryptographiques et des longueurs de clé classés comme sûrs. L'établissement de santé se conforme à cet égard à la directive technique TR-02102 du BSI [R01].
08.02	Surveillance des erreurs de transmission : Lors d'un transfert de données vers un système central de l'établissement de santé (par ex. PACS), les erreurs de transmission sont détectées. Les utilisateurs ou le service informatique compétent de l'établissement de santé [R03] sont immédiatement informés.
08.03	Chiffrement : Toutes les communications internes et externes à l'origine et à destination du système sont chiffrées à l'aide de protocoles de communication sécurisés.
08.04	Fonctions de routage : Le système ne permet aucune fonctionnalité de pontage, de routage ou autre fonctionnalité de transfert vers d'autres segments du réseau. Les fonctions correspondantes sont désactivées.
08.05	Adressage réseau : Le système prend en charge un adressage réseau configurable, qui peut ainsi être défini par l'établissement de santé.
08.06	Liaisons de communication par câble : Les liaisons de communication filaires sont établies exclusivement via l'infrastructure réseau de l'établissement de santé. Un système connecté au réseau prend en charge l'authentification par port selon la norme 802.1x au moyen du protocole EAP-TLS ou d'alternatives équivalentes approuvées par le service informatique de l'établissement de santé [R03].
08.07	Liaisons de communication sans fil (WLAN) : Pour les communications sans fil, seuls les composants réseau de l'établissement de santé sont utilisés. La norme de chiffrement minimale est WPA2 Enterprise, et le protocole d'authentification EAP-TLS. Des solutions alternatives équivalentes peuvent être utilisées si elles sont approuvées par le service informatique de l'établissement de santé [R03].
08.08	Connexions par bluetooth : Si des connexions Bluetooth sont nécessaires, celles-ci doivent correspondre au moins au mode de sécurité 4 niveau 4 pour Bluetooth Classic et au mode de sécurité 1 niveau 4 pour Bluetooth LE.
08.09	Connexions internet sortantes : Lorsque des connexions internet sont nécessaires, elles doivent impérativement passer le proxy web de l'établissement de santé. Le système dispose pour cela d'une fonctionnalité proxy.
08.10	Synchronisation des heures système : Le système prend en charge le protocole réseau NTP pour la synchronisation de l'heure système. Réf. MDS2 : AUDT-4.1.1

2.9 Gestion des accès

ID	Exigence
09.01	Séparation des comptes pour les services système : Les comptes de service (comptes pour les services système) sont séparés des comptes utilisateurs. Ils disposent exclusivement

ID	Exigence
	des autorisations nécessaires au fonctionnement des services système prévus (principe de privilège minimal). Réf. MDS2 : AUTH-2
09.02	Utilisation de comptes administrateurs locaux : Les comptes administrateurs locaux sont utilisés exclusivement pour la maintenance et la configuration. L'utilisation professionnelle s'effectue via des comptes utilisateurs personnels.
09.03	Authentification des accès : L'accès au système nécessite toujours une authentification. Tous les comptes utilisateurs sont protégés par des mécanismes d'authentification appropriés. Réf. MDS2 : AUTH-1
09.04	Authentification au niveau des interfaces : La transmission des données via des interfaces s'effectue exclusivement de manière authentifiée. L'authentification concerne au minimum le système émetteur et le système récepteur. Les informations d'authentification (mots de passe, clés, etc.) sont conservées de manière à être protégées contre tout accès non autorisé.
09.05	Règles concernant les mots de passe : Les mots de passe par défaut sont modifiés conformément aux directives de l'établissement de santé [R03] avant la mise en service opérationnelle. Il convient de s'assurer que les mots de passe utilisés sont générés spécifiquement pour chaque établissement de santé et ne sont pas utilisés par d'autres clients. Si des tiers non autorisés sont susceptibles d'avoir eu connaissance de ces mots de passe, le fournisseur de l'établissement de santé le signale immédiatement et les mots de passe sont modifiés dans les systèmes concernés. Réf. MDS2 : PAUT-6
09.06	Gestion des informations d'accès : Les informations d'accès (par ex. mots de passe, clés numériques ou physiques) sont classées comme secrètes et traitées et protégées comme telles par le fournisseur et ses systèmes. Elles sont modifiées régulièrement, à des intervalles à définir [R03].
09.07	Autorisations : Le système dispose d'autorisations basées sur les rôles ou un mécanisme similaire. Réf. MDS2 : AUTH-2
09.08	Octroi d'autorisations : Le système prend en charge la connexion du système IAM de l'établissement de santé via une interface standardisée pour l'octroi des autorisations. Réf. MDS2 : PAUT-2
09.09	Blocage de la session utilisateur en cas d'inactivité : Le système permet à l'utilisateur de verrouiller manuellement sa session (par ex. lorsqu'il quitte le système). Une session utilisateur est automatiquement verrouillée après une période d'inactivité définie par l'établissement de santé [R03]. Réf. MDS2 : ALOF-1
09.10	Federated identity : L'authentification des utilisateurs et la transmission des informations nécessaires à l'accès aux ressources s'effectuent via une relation de confiance (*trust*) entre le système et l'infrastructure prévue à cet effet par l'établissement de santé (identité fédérée). Réf. MDS2 : PAUT-2

2.10 Maintenance et assistance

ID	Exigence
10.01	Accès à distance : Les fournisseurs qui ont besoin d'un accès à distance au système de l'établissement de santé respectent les consignes de sécurité nécessaires et utilisent exclusivement les systèmes d'accès à distance de l'établissement de santé [R03]. L'accès à distance doit se faire via des comptes utilisateurs personnels. Les systèmes d'accès à distance propres aux fournisseurs ne sont pas acceptés par l'établissement de santé. Réf. MDS2 : RMOT-1 | Réf. MDS2 : RMOT-2 | Réf. MDS2 : RMOT-3
10.02	Annonce préalable des travaux de maintenance : Les travaux de maintenance effectués par le fournisseur, qu'ils soient réalisés sur place ou à distance, doivent être signalés au préalable au service spécialisé et au service informatique de l'établissement de santé [R03]. Si des circonstances particulières exigent des travaux de maintenance immédiats, ceux-ci sont signalés dans les 24 heures qui suivent au service spécialisé et au service informatique, avec justification claire de l'urgence.
10.03	Travaux de maintenance à l'aide de supports amovibles : Le raccordement de supports amovibles aux systèmes de l'établissement de santé (y c. les systèmes fournis par le fournisseur) n'est pas autorisé. Les supports amovibles destinés au transfert ou à la sauvegarde de données sont fournis par l'établissement de santé. Le fournisseur met à la disposition du personnel informatique de l'établissement de santé les logiciels nécessaires à la réalisation de ces travaux au moins deux semaines avant la maintenance. Le personnel de l'établissement de santé vérifie les logiciels et les met à la disposition du fournisseur sur un support approprié fourni par l'établissement de santé afin qu'il puisse effectuer la maintenance.

3 Références

#	Désignation	Référence
R01	BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (en allemand et anglais)	Lien
R02	Manufacturer Disclosure Statement for Medical Device Security (version de 2019 ; en anglais)	Lien
R03	Normes appliquées et stratégie informatique ainsi que les points de contact de l'établissement de santé. Ce document est transmis directement par l'établissement de santé aux fournisseurs.	Annexe de l'établissement de santé
R04	DIN 66399-1 Büro- und Datentechnik - Vernichten von Datenträgern 8en allemand et anglais)	Lien

Dernière vérification des références le 2.2.2026.