Trustteam

Statement Of Applicability

D-MSP-002.3

Date de création: 04/03/2018

Date de révision: 28/04/2022

N°	Clausule ISO/IEC 27001:2013 Annex A controls / Exigences HDS	Controle	Applicable?	raison de l'exclusion	Explication ou référence au contrôle
A.5 Politique de sécurité					
A.5.1 Politique de sécurité de l'information					
A.5.1.1	Document de politique de sécurité de l'information	Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.	oui		Est appliqué
A.5.1.2	Revue des politiques de sécurité de l'information	Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur perti- nence, leur adéquation et leur effectivité dans le temps.	oui		Est appliqué
A.6 Organisation de la sécurité de l'information					
A.6.1 Organisation interne					
A.6.1.1	Fonctions et responsabilités liées à la sécurité de l'information	Toutes les responsabilités en matière de sécurité de l'information doivent être définies et attribuées.	oui		Est appliqué
A.6.1.2	Séparation des tâches	Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.	oui		Est appliqué
A.6.1.3	Relations avec les autorités	Des relations appropriées avec les autorités compétentes doivent être entretenues.	oui		Est appliqué
A.6.1.4	Relations avec des groupes de spécialisés	Des relations appropriées avec des groupes d'intérêt, des forums spécia- lisés dans la sécurité et des associations professionnelles doivent être entretenues.	oui		Est appliqué
A.6.1.5	La sécurité de l'information dans la gestion de projet	La sécurité de l'information doit être considérée dans la gestion de projet, quel que soit le type de projet concerné.	oui		Est appliqué
A.6.2 Appareils mobiles et télétravail					
A.6.2.1	Politique en matière d'appareils mobiles	Une politique et des mesures de sécurité complémentaires doivent être adoptées pour gérer les risques découlant de l'utilisation des appareils mobiles.	oui		Est appliqué
A.6.2.2	Télétravail	Une politique et des mesures de sécurité complémentaires doivent être mises en œuvre pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.	oui		Est appliqué
A.7 Sécurité des ressources humaines					
A.7.1 Avant embauche					

A.7.1.1	Sécurité des ressources humaines	Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.	oui		Est appliqué
A.7.1.2	Avant embauche	Les accords contractuels entre les salariés et les sous-traitants doivent préciser leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.	oui		Est appliqué
A.7.2 Pendant la durée du contrat					
A.7.2.1	Responsibilités de la direction	La direction doit demander à tous les salariés et sous-traitants d'appliquer les règles de sécurité de l'information conformément aux politiques et aux procédures en vigueur dans l'organisation.	oui		Est appliqué
A.7.2.2	Sensibilisation, apprentissage et formations à la sécurité de l'information	L'ensemble des salariés de l'organisation et, quand cela est pertinent, des sous-traitants, doit bénéficier d'une sensibilisation et de formations adaptées et recevoir régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.	oui		Est appliqué
A.7.2.3	Processus disciplinaire	Un processus disciplinaire formel et connu de tous doit exister pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.	oui		Est appliqué
A.7.3 Rupture, terme ou modification du contrat de travail					
A.7.3.1	Achèvement ou modification des responsabilités associées au contrat de travail	Les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, doivent être définies, communiquées au salarié ou au sous-traitant, et appliquées.	oui		Est appliqué
A.8 Gestion des actifs/biens					
A.8.1 Responsabilités relatives aux actifs					
A.8.1.1	Inventaire des actifs	Les actifs associés à l'information et aux moyens de traitement de l'information doivent être identifiés et un inventaire de ces actifs doit être dressé et tenu à jour.	oui		Est appliqué
A.8.1.2	Propriété des actifs	Les actifs figurant à l'inventaire doivent être attribués à un propriétaire.	oui		Est appliqué
A.8.1.3	Utilisation correcte des actifs	Les règles d'utilisation correcte de l'information, les actifs associés à l'infor- mation et les moyens de traitement de l'information doivent être identifiés, documentés et mis en œuvre.	oui		Est appliqué
A.8.1.4	Retours des actifs	Tous les salariés et les utilisateurs tiers doivent restituer la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord.	oui		Est appliqué

A.8.2 Classification des informations					
A.8.2.1	Classification des informations	Les informations doivent être classifiées en termes d'exigences légales, de valeur, de caractère critique et de sensibilité au regard d'une divulgation ou modification non autorisée.	oui		Est appliqué
A.8.2.2	Marquage et manipulation de l'information	Un ensemble approprié de procédures pour le marquage de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisation.	oui		Est appliqué
A.8.2.3	Manipulation des actifs	Des procédures de traitement de l'information doivent être élaborées et mises en œuvre conformément au plan de classification de l'information adopté par l'organisation.	oui		Est appliqué
A.8.3 Manipulation des supports					
A.8.3.1	Gestion des supports amovibles	Des procédures de gestion des supports amovibles doivent être mises en œuvre conformément au plan de classification adopté par l'organisation.	oui		Est appliqué
A.8.3.2	Mise au rebut des supports	Les supports qui ne sont plus nécessaires doivent être mis au rebut de manière sécurisée en suivant des procédures formelles.	oui		Est appliqué
A.8.3.3	Transfert physique des supports	Les supports contenant de l'information doivent être protégés contre les accès non autorisés, les erreurs d'utilisation et l'altération lors du transport.	oui		Est appliqué
A.9 Gestion des accès					
A.9.1 Exigences métier en matière de contrôle d'accès					
A.9.1.1	Politique de contrôle d'accès	Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information.	oui		Est appliqué
A.9.1.2	Accès aux réseaux et aux services réseaux	Les utilisateurs doivent avoir uniquement accès au réseau et aux services réseau pour lesquels ils ont spécifiquement reçu une autorisation.	oui		Est appliqué
A.9.2 Gestion de l'accès utilisateur					
A.9.2.1	Enregistrement et désinscription des utilisateurs	Un processus formel d'enregistrement et de désinscription des utilisateurs doit être mis en œuvre pour permettre l'attribution des droits d'accès.	oui		Est appliqué
A.9.2.2	Distribution des accès aux utilisateurs	Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d'accès à tous types d'utilisa- teurs sur l'ensemble des services et des systèmes.	oui		Est appliqué
A.9.2.3	Gestion des droits d'accès à privilèges	L'allocation et l'utilisation des droits d'accès à privilèges doivent être restreintes et contrôlées.	oui		Est appliqué
A.9.2.4	Gestion des informations secrètes d'authentification des utilisateurs	L'attribution des informations secrètes d'authentification doit être réalisée dans le cadre d'un processus de gestion formel.	oui		Est appliqué
A.9.2.5	Revue des droits d'accès utilisateurs	Les propriétaires d'actifs doivent vérifier les droits d'accès des utilisateurs à intervalles réguliers.	oui		Est appliqué

A.9.2.6	Suppression ou adaptation des droits d'accès	Les droits d'accès aux informations et aux moyens de traitement des infor- mations de l'ensemble des salariés et utilisateurs tiers doivent être suppri- més à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord.	oui		Est appliqué
A.9.3 Responsabilités de l'utilisateur					
A.9.3.1	Utilisation d'informations secrètes d'authentification	Gebruikers zijn verplicht om de praktijken van de organisatie te volgen in het gebruik van geheime identificatie-informatie.	oui		Est appliqué
A.9.4 Contrôle de l'accès au système et à l'information					
A.9.4.1	Restriction d'accès à l'information	L'accès à l'information et aux fonctions d'application système doit être res- treint conformément à la politique de contrôle d'accès.	oui		Est appliqué
A.9.4.2	Sécuriser les procédures de connexion	Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.	oui		Est appliqué
A.9.4.3	Système de gestion des mots de passe	Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent garantir la qualité des mots de passe.	oui		Est appliqué
A.9.4.4	Utilisation de programmes utilitaires privilèges	L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée.	oui		Est appliqué
A.9.4.5	Contrôle d'accès au code source des programmes	L'accès au code source des programmes doit être restreint.	oui		Est appliqué
A.10	Cryptografie				
A.10.1	Cryptografische controles				
A.10.1.1	Politique d'utilisation des mesures cryptographiques	Une politique d'utilisation des mesures cryptographiques en vue de proté- ger l'information doit être élaborée et mise en œuvre.	oui		Est appliqué
A.10.1.2	Gestions des clés	Une politique sur l'utilisation, la protection et la durée de vie des clés cryp- tographiques doit être élaborée et mise en œuvre tout au long de leur cycle de vie.	oui		Est appliqué
A.11 Sécurité physique et environnementale					
A.11.1 Zones sécurisées					
A.11.1.1	Périmètre de sécurité physique	Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traite- ment de l'information.	oui		Est appliqué
A.11.1.2	Contrôle d'accès physique	Les zones sécurisées doivent être protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.	oui		Est appliqué
A.11.1.3	Sécurisation des bureaux, des salles et des équipements	Des mesures de sécurité physique aux bureaux, aux salles et aux équipe- ments doivent être conçues et appliquées.	oui		Est appliqué
A.11.1.4	Protection contre les menaces exterieures et environnemntales	Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être conçues et appliquées.	oui		Est appliqué

A.11.1.5	Travail dans les zones sécurisées	Des procédures pour le travail dans les zones sécurisées doivent être conçues et appliquées.	oui		Est appliqué
A.11.1.6	Zones de livraison et chargement	Les points d'accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux doivent être contrôlés et, si possible, isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.	oui		Est appliqué
A.11.2 Matériels					
A.11.2.1	Emplacement et protection des matériels	Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibi- lités d'accès non autorisé.	oui		Est appliqué
A.11.2.2	Services généraux	Les matériels doivent être protégés des coupures de courant et autres per- turbations dues à une défaillance des services généraux.	oui		Est appliqué
A.11.2.3	Sécurité du câblage	Les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information doivent être protégés contre toute interception ou tout dommage.	oui		Est appliqué
A.11.2.4	Maintenance des matériels	Les matériels doivent être entretenus correctement pour garantir leur dis- ponibilité permanente et leur intégrité.	oui		Est appliqué
A.11.2.5	Sortie des actifs	Les matériels, les informations ou les logiciels des locaux de l'organisation ne doivent pas sortir sans autorisation préalable.	oui		Est appliqué
A.11.2.6	Sécurité des matériels et actifs hors des locaux	Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de l'organisation en tenant compte des différents risques asso- ciés au travail hors site.	oui		Est appliqué
A.11.2.7	Mise au rebut ou recyclage sécurisé(e) du matériel	Tous les composants des matériels contenant des supports de stockage doivent être vérifiés pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant leur mise au rebut ou leur réutilisation.	oui		Est appliqué
A.11.2.8	Matériels utilisateur laissés sans surveillance	Les utilisateurs doivent s'assurer que les matériels non surveillés sont dotés d'une protection appropriée.	oui		Est appliqué
A.11.2.9	Politique du bureau propre et de l'écran vérrouillé	Une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran verrouillé pour les moyens de traitement de l'information doivent être adoptées.	oui		Est appliqué
A.12 Sécurité liée à l'exploitation					
A.12.1 Procédures et responsabilités liées à l'exploitation					
A.12.1.1	Procédures d'exploitation documentées	Les procédures d'exploitation doivent être documentées et mises à disposi- tion de tous les utilisateurs concernés.	oui		Est appliqué

A.12.1.2	Gestion des changements	Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sur la sécurité de l'information doivent être contrôlés.	oui		Est appliqué
A.12.1.3	Dimensionnement	L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système.	oui		Est appliqué
A.12.1.4	Séparation des environnements de développement, de test et d'exploitation	Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non auto- risés dans l'environnement en exploitation.	oui		Est appliqué
A.12.2 Protection contre les logiciels malveillants					
A.12.2.1	Mesures contre les logiciels malveillants	Des mesures de détection, de prévention et de récupération conjuguées à une sensibilisation des utilisateurs adaptée, doivent être mises en œuvre pour se protéger contre les logiciels malveillants.	oui		Est appliqué
A.12.3 Sauvegarde					
A.12.3.1	Sauvegarde des informations	Des copies de sauvegarde de l'information, des logiciels et des images systèmes doivent être réalisés et testés régulièrement conformément à une politique de sauvegarde convenue.	oui		Est appliqué
A.12.4 Journalisation et surveillance					
A.12.4.1	Journalisation des évènements	Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'informa- tion doivent être créés, tenus à jour et vérifiés régulièrement.	oui		Est appliqué
A.12.4.2	Protection de l'information journalisée	Les moyens de journalisation et d'information journalisée doivent être pro- tégés contre les risques de falsification ou d'accès non autorisé.	oui		Est appliqué
A.12.4.3	Journaux d'administrateur et opérateur	Les activités de l'administrateur système et de l'opérateur système doivent être journalisées, protégées et vérifiées régulièrement.	oui		Est appliqué
A.12.4.4	Synchronisation des horloges	Les horloges de l'ensemble des systèmes de traitement de l'information concernés d'une organisation ou d'un domaine de sécurité doivent être synchronisées sur une source de référence temporelle unique.	oui		Est appliqué
A.12.5 Maîtrise des logiciel en exploitation					
A.12.5.1	Installation de logiciels sur des systèmes en exploitation	Des procédures doivent être mises en œuvre pour contrôler l'installation de logiciel sur des systèmes en exploitation.	oui		Est appliqué
A.12.6 Gestion des vulnérabilités techniques					

A.12.6.1	Gestion des vulnérabilités techniques	Des informations sur les vulnérabilités techniques des systèmes d'informa- tion en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appro- priées doivent être prises pour traiter le risque associé.	oui		Est appliqué
A.12.6.2	Restrictions liées à l'installation de logiciels	Des règles régissant l'installation de logiciels par les utilisateurs doivent être établies et mises en œuvre.	oui		Est appliqué
A.12.7 Considérations sur l'audit des systèmes d'information					
A.12.7.1	Mesures relatives à l'audit des systèmes d'information	Les exigences et activités d'audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations subies par les processus métier.	oui		Est appliqué
A.13 Sécurité des communications					
A.13.1 Gestion de la sécurité des réseaux					
A.13.1.1	Contrôle des réseaux	Les réseaux doivent être gérés et contrôlés pour protéger l'information contenue dans les systèmes et les applications.	oui		Est appliqué
A.13.1.2	Sécurité des services de réseaux	Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.	oui		Est appliqué
A.13.1.3	Cloisonnement des réseaux	Les groupes de services d'information, d'utilisateurs et de systèmes d'infor- mation doivent être cloisonnés sur les réseaux.	oui		Est appliqué
A.13.2 Transfert de l'information					
A.13.2.1	Politiques et procédures de transfert de l'information	Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information tran- sitant par tous types d'équipements de communication.	oui		Est appliqué
A.13.2.2	Accords en matière de transfert de l'information	Des accords doivent traiter du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers.	oui		Est appliqué
A.13.2.3	Messagerie électronique	L'information transitant par la messagerie électronique doit être protégée de manière appropriée.	oui		Est appliqué
A.13.2.4	Engagements de confidentialité ou de non-divulgation	Les exigences en matière d'engagements de confidentialité ou de non-divul- gation, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l'organisation.	oui		Est appliqué
A.14 Acquisition, développement et maintenance des systèmes d'information					
A.14.1 Exigences de sécurité applicables aux systèmes d'information					
A.14.1.1	Analyse et spécifications des exigences de sécurité de l'information	Les informations doivent être classifiées en termes d'exigences légales, de valeur, de caractère critique et de sensibilité au regard d'une divulgation ou modification non autorisée.	oui		Est appliqué

A.14.1.2	Sécurisation des services d'application sur les réseaux publics	Un ensemble approprié de procédures pour le marquage de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisation.	oui		Est appliqué
A.14.1.3	Protection des transactions liées aux services d'application	Des procédures de traitement de l'information doivent être élaborées et mises en œuvre conformément au plan de classification de l'information adopté par l'organisation.	oui		Est appliqué
A.14.2 Sécurité des processus de développement et d'assistance technique					
A.14.2.1	Politique de développement sécurisé	Des règles de développement des logiciels et des systèmes doivent être établies et appliquées aux développements de l'organisation.	oui		Est appliqué
A.14.2.2	Procédures de contrôle des changements de système	Les changements des systèmes dans le cadre du cycle de développement doivent être contrôlés par le biais de procédures formelles.	oui		Est appliqué
A.14.2.3	Revue technique des appplications après changement apporté à la plateforme d'exploitation	Lorsque des changements sont apportés aux plateformes d'exploitation, les applications critiques métier doivent être vérifiées et testées afin de véri- fier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.	oui		Est appliqué
A.14.2.4	Restrictions relatives aux changements apportés aux progiciels	Les modifications des progiciels ne doivent pas être encouragées, être limi- tées aux changements nécessaires et tout changement doit être strictement contrôlé.	oui		Est appliqué
A.14.2.5	Principes d'ingénieurie de la sécurité des systèmes	Des principes d'ingénierie de la sécurité des systèmes doivent être établis, documentés, tenus à jour et appliqués à tous les travaux de mise en œuvre des systèmes d'information.	oui		Est appliqué
A.14.2.6	Environnement de développement sécurisé	Les organisations doivent établir des environnements de développement sécurisés pour les tâches de développement et d'intégration du système, qui englobe l'intégralité du cycle de vie du développement du système, et en assurer la protection de manière appropriée.	oui		Est appliqué
A.14.2.7	Développement externalisé	L'organisation doit superviser et contrôler l'activité de développement du système externalisée.	oui		Est appliqué
A.14.2.8	Test de la sécurité du système	Les tests de fonctionnalité de la sécurité doivent être réalisés pendant le développement.	oui		Est appliqué
A.14.2.9	Test de conformité du système	Des programmes de test de conformité et des critères associés doivent être déterminés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.	oui		Est appliqué
A.14.3 Données de test					
A.14.3.1	Protection des données de test	Les données de test doivent être sélectionnées avec soin, protégées et contrôlées.	oui		Est appliqué
A.15 Relations avec les fournisseurs					
A.15.1 Sécurité dans les relations avec les fournisseurs					

A.15.1.1	Politique de sécurité de l'information dans les relations avec les fournisseurs	Des exigences de sécurité de l'information pour limiter les risques résultant de l'accès des fournisseurs aux actifs de l'organisation doivent être accep- tées par le fournisseur et documentées.	oui		Est appliqué
A.15.1.2	La sécurité dans les accords conclus avec les fournisseurs	Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.	oui		Est appliqué
A.15.1.3	Chaîne d'approvisionnement des produits et des services informatiques	Les accords conclus avec les fournisseurs doivent inclure des exigences sur le traitement des risques liés à la sécurité de l'information associé à la chaîne d'approvisionnement des produits et des services informatiques.	oui		Est appliqué
A.15.2 Gestion de la prestation du service					
A.15.2.1	Surveillance et revue des services fournisseurs	Les organisations doivent surveiller, vérifier et auditer à intervalles régu- liers la prestation des services assurés par les fournisseurs.	oui		Est appliqué
A.15.2.2	Gestion des changements apportées dans les services des fournisseurs	Les changements effectués dans les prestations de service des fournisseurs, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation des risques.	oui		Est appliqué
A.16 Gestion des incidents liés à la sécurité de l'information					
A.16.1 Gestion des incidents liés à la sécurité de l'information et améliorations					
A.16.1.1	Responsabilités et procédures	Des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente doivent être établies en cas d'incident lié à la sécurité de l'information.	oui		Est appliqué
A.16.1.2	Signalement des événements liés à la sécurité de l'information	Les événements liés à la sécurité de l'information doivent être signalés dans les meilleurs délais par les voies hiérarchiques appropriées.	oui		Est appliqué
A.16.1.3	Signalement des failles liées à la sécurité de l'information	Les salariés et les sous-traitants utilisant les systèmes et services d'infor- mation de l'organisation doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.	oui		Est appliqué
A.16.1.4	Appréciation des évènements liés à la sécurité de l'information et prise de décision	Les événements liés à la sécurité de l'information doivent être appréciés et il doit être décidé s'il faut les classer comme incidents liés à la sécurité de l'information.	oui		Est appliqué
A.16.1.5	Réponse aux incidents liées à la sécurité de l'information	Les incidents liés à la sécurité de l'information doivent être traités confor- mément aux procédures documentées.	oui		Est appliqué

A.16.1.6	Tirer des enseignements des incidents liés à la sécurité de l'information	Les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.	oui		Est appliqué
A.16.1.7	Collecte de preuves	L'organisation doit définir et appliquer des procédures d'identification, de collecte, d'acquisition et de protection de l'information pouvant servir de preuve.	oui		Est appliqué
A.17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité					
A.17.1 Continuité de la sécurité de l'information					
A.17.1.1	Organisation de la continuité de la sécurité de l'information	L'organisation doit déterminer ses exigences en matière de sécurité de l'in- formation et de continuité de management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre	oui		Est appliqué
A.17.1.2	Mise en œuvre de la continuité de la sécurité de l'information	L'organisation doit établir, documenter, mettre en œuvre et tenir à jour des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de sécurité de l'information au cours d'une situation défavorable.	oui		Est appliqué
A.17.1.3	Vérifier, revoir et évaluer la continuité de la sécurité de l'information	L'organisation doit vérifier les mesures de continuité de la sécurité de l'information mises en œuvre à intervalles réguliers afin de s'assurer qu'elles sont valables et efficaces dans des situations défavorables.	oui		Est appliqué
A.17.2 Redondances					
A.17.2.1	Disponibilité des moyens de traitement de l'information	Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.	oui		Est appliqué
A.18 Conformité					
A.18.1 Conformité aux obligations légales et réglementaires					
A.18.1.1	Identification de la legislation et des exigences contractuelles applicables	Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour pour chaque système d'information et pour l'organisation elle-même.	oui		Est appliqué
A.18.1.2	Droits de propriété intellectuelle	Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires.	oui		Est appliqué
A.18.1.3	Protection des enregistrements	Les enregistrements doivent être protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.	oui		Est appliqué

A.18.1.4	Protection de la vie privée et protection des données à caractère personnel	La protection de la vie privée et la protection des données à caractère personnel doivent être garanties telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.	oui		Est appliqué
A.18.1.5	Réglementation relative aux mesures cryptographiques	Des mesures cryptographiques doivent être prises conformément aux accords, législation et réglementations applicables.	oui		Est appliqué
A.18.2 Revue de la sécurité de l'information					
A.18.2.1	Revue indépendante de la sécurité de l'information	Des revues régulières et indépendantes de l'approche retenue par l'organisme pour gérer et mettre en œuvre la sécurité de l'information (à savoir le suivi des objectifs de sécurité, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effec- tuées à intervalles définis ou lorsque des changements importants sont intervenus.	oui		Est appliqué
A.18.2.2	Conformité avec les politiques et les normes de sécurité	Les responsables doivent régulièrement vérifier la conformité du traitement de l'information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité.	oui		Est appliqué
A.18.2.3	Vérification de la conformité technqiue	Les systèmes d'information doivent être examinés régulièrement quant à leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation.	oui		Est appliqué
HDS - Hébergement de données de santé					
HDS 4.2. Exigences NF ISO 27001					
ISO 27001 complet	Les hébergeurs d'infrastructure physique et les hébergeurs infogéreurs doivent être certifiés NF ISO 27001		oui		Est appliqué

ISO 27001 - 4.3 supplémentaire	L'hébergeur doit déterminer le domaine d'application du SMSI en tenant compte de l'objectif de protection des données de santé à caractère personnel en plus des enjeux et exigences déjà considérés.	Ce domaine d'application doit au moins couvrir l'ensemble des activités d'hébergement de données de santé à caractère personnel de l'hébergeur	oui		Est appliqué
ISO 27001 - 6.1.3 suppl.	La DdA (déclaration d'applicabilité) du SMSI doit inclure l'ensemble des exigences du référentiel de certification HDS	Toute exclusion d'exigences, du périmètre de certification, doit être formellement justifiée et la justification doit être approuvée par l'organisme de certification	oui		Est appliqué
ISO 27001 Annexe A12.3 supplém.	En cas d'externalisation des sauvegardes de données de santé, quel qu'en soit le support, l'hébergeur doit en garantir la sécurité	Le SMSI prend en compte les sauvegardes de données de santé, notamment leur sécurité sur les critères de confidentialité, intégrité et traçabilité lors des transferts et pendant leur conservation Les mesures de sécurité des sauvegardes sont mises en œuvre.	oui		Est appliqué
ISO 27001 Annexe A12.7 supplém.	L'hébergeur doit permettre à ses clients d'effectuer des audits sur les applications mises en production	• S'assurer que l'hébergeur infogéreur a défini, documenté et mis en œuvre une procédure encadrant la réalisation des audits de ses clients, en particulier les audits de sécurité (test d'intrusion, etc.) ; • Les éléments relevant de la responsabilité de l'hébergeur, en particulier des éléments mutualisés, peuvent être exclus du périmètre d'audit des clients ; dans ce cas, il convient de s'assurer que l'hébergeur est en mesure de fournir à ses clients les résultats d'un audit externe indépendant sur ces éléments	oui		Est appliqué
HDS 4.3. Exigences NF ISO 20000-1					
HDS 4.3.1. Planification de nouveaux services ou de services modifiés					

ISO 20000-1 5.2.	Planifier des services nouveaux ou modifiés	Le fournisseur de services doit identifier les exigences de service pour les services nouveaux ou modifiés. Les services nouveaux ou modifiés services nouveaux ou modifiés doivent être planifiés de manière à répondre aux exigences de service. La planification des services nouveaux ou modifiés doit être convenue avec le client et les parties intéressées	oui		Est appliqué
HDS 4.3.2. Conception et implémentation des nouveaux services ou des services modifiés					
ISO 20000-1 5.3.b - HDS 4.3.2.1	HDS 4.3.2.1. Présentation des activités exécutées par les fournisseurs de services, clients et autres parties	5.3.Conception et développement de services nouveaux ou modifiés b). les activités à réaliser par le prestataire de services, le client et les autres parties pour la fourniture des nouveaux services ou des services modifiés	oui		Est appliqué
ISO 20000-1 5.3.b supplém. HDS 4.3.2.1	L'hébergeur doit définir des critères d'acceptation pour tout nouveau service ou pour toute modification de service et réaliser des tests d'acception avant leur mise en production	• S'assurer que l'hébergeur infogéreur a mis en place une méthodologie de vérification des applications qu'il héberge ; • Vérifier que l'hébergeur infogéreur a formalisé une procédure permettant de définir les prérequis à l'hébergement et une procédure de vérification de ces prérequis (ces prérequis doivent comporter, a minima, le manuel d'installation et le manuel d'exploitation) ; • Vérifier que l'hébergeur infogéreur a formalisé un processus structuré de test et de validation permettant d'apporter la preuve objective que le futur service ne perturbera pas les performances globales du système hébergé et n'amoindrira pas son niveau de sécurité	oui		Est appliqué
HDS 4.3.3. Continuité de services et gestion de la disponibilité					
4.3.3.1.	Le chapitre 6.3 de la norme NF ISO 20000-1 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs 6.3. Gestion de la continuité et de la disponibilité des services	6.3.1 Exigences en matière de continuité et de disponibilité des services	oui		Est appliqué

4.3.3.1.?	Le chapitre 6.3 de la norme NF ISO 20000-1 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs 6.3. Gestion de la continuité et de la disponibilité des services 6.3.2 Plans de continuité et de disponibilité des services	Le fournisseur de services doit créer, mettre en œuvre et maintenir un ou plusieurs plans de continuité des services et un ou plusieurs plans de disponibilité. de disponibilité. Les modifications de ces plans doivent être contrôlées par le processus de gestion des changements. Le ou les plans de disponibilité doivent comprendre au moins des exigences et des objectifs de disponibilité. Le fournisseur de services doit évaluer l'impact des demandes de changement sur le(s) plan(s) de continuité des services et le(s) plan(s) de disponibilité.	oui		Est appliqué
4.3.3.1.?	Le chapitre 6.3 de la norme NF ISO 20000-1 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs 6.3. Gestion de la continuité et de la disponibilité des services 6.3.3 Surveillance et tests de la continuité et de la disponibilité des services	La disponibilité des services est contrôlée, les résultats sont enregistrés et comparés aux objectifs convenus. Les indisponibilités non planifiées Les indisponibilités imprévues font l'objet d'une enquête et les mesures nécessaires sont prises. Les plans de continuité des services doivent être testés par rapport aux exigences de continuité des services. Les plans de disponibilité doivent être Les plans de disponibilité sont testés par rapport aux exigences de disponibilité. Les plans de continuité et de disponibilité du service doivent être testés de nouveau après après des changements majeurs de l'environnement de service dans lequel le fournisseur de services opère. Les résultats des tests doivent être enregistrés. Des examens doivent être effectués après chaque test et après le déclenchement du plan de continuité du service. plan de continuité du service a été invoqué. En cas de déficiences, le prestataire de services prend les mesures nécessaires et rend compte de ces mesures. nécessaires et rend compte des mesures prises	oui		Est appliqué

4.3.3.2.	Le chapitre 6.5 de la norme NF ISO 20000-1 s'applique aux hébergeurs d'infrastructure physique et aux hébergeurs infogéreurs. Gestion de capacité.	Le fournisseur de services identifie et convient avec le client et les parties intéressées des exigences en matière de capacité et de performance parties intéressées. Le fournisseur de services doit créer, mettre en œuvre et maintenir un plan de capacité en tenant compte des ressources humaines, techniques, informationnelles et financières, techniques, d'information et financières. Les modifications apportées au plan de capacité sont contrôlées par le processus de gestion du changement. processus de gestion du changement. Le plan de capacité comprend au moins les éléments suivants a) la demande actuelle et prévisionnelle de services ; b) l'impact attendu des exigences convenues en matière de disponibilité, de continuité du service et de niveaux de service ; c) les calendriers, les seuils et les coûts des améliorations de la capacité des services ; d) l'impact potentiel des changements statutaires, réglementaires, contractuels ou organisationnels ; e) l'impact potentiel des nouvelles technologies et des nouvelles techniques ; f) les procédures permettant une analyse prédictive, ou la référence à celles-ci. Le fournisseur de services surveille l'utilisation de la capacité, analyse les données relatives à la capacité et ajuste les performances. Le prestataire de services fournisseur de services fournit une capacité suffisante pour répondre aux exigences convenues en matière de capacité et de	oui		Est appliqué
HDS 4.4. Exigences relatives à la protection des données de santé à caractère personnel					
HDS 4.4.1. Droits des personnes					
4.4.1.1.	Obligation de coopérer	L'hébergeur doit mettre à disposition les procédures et moyens pour permettre à ses clients de répondre aux demandes d'exercice des droits des personnes concernées. Les droits couverts sont ceux définis par les articles 15 à 2+C1932 du règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016	oui		Est appliqué
HDS 4.4.2. Finalité					
4.4.2.1.	L'hébergeur traite les données à caractère personnel uniquement sur instruction documentée du client et ne doit pas déroger aux finalités précisées dans les instructions.	Ces instructions doivent être documentées dans le cadre du contrat passé avec le client.	oui		Est appliqué

4.4.2.1.	L'hébergeur ne doit pas utiliser les données de santé qu'il héberge à d'autres fins que l'exécution de la prestation d'hébergement.	Est notamment interdite, toute utilisation de ces données à des fins marketings, publicitaires, commerciales, ou statistiques.	oui		Est appliqué
HDS 4.4.3. Communication des données					
4.4.3.1.	Données temporaires	L'hébergeur doit définir une période de rétention des données temporaires et respecter ce délai. L'hébergeur doit documenter et mettre en place les moyens permettant de s'assurer que les données temporaires sont effacées à expiration de ce délai.	oui		Est appliqué
4.4.3.2.	Notification en cas de communication de données à caractère personnel	Les saisies judiciaires incluant des données à caractère personnel doivent être encadrées au niveau contractuel. Une procédure doit définir les modalités de notification du client d'une telle transmission, sauf à ce que cette notification soit interdite.	oui		Est appliqué
4.4.3.3.	Traçabilité en cas de communication	L'hébergeur doit assurer la journalisation de la transmission des données à caractère personnel à des tiers avec a minima les informations suivantes : la liste des données transmises, le ou les destinataires et les dates de communication.	oui		Est appliqué
4.4.3.4.	Intégrité et acquittement des échanges	Les données à caractère personnel transitant par un réseau de communication doivent faire l'objet de contrôles permettant de s'assurer que ces données sont bien reçues par le système cible.	oui		Est appliqué
HDS 4.4.4. Transparence					
4.4.4.1.	Obligation d'information en cas de sous-traitance	Les clauses contractuelles passées entre l'hébergeur et son client doivent préciser le recours éventuel à un sous-traitant dans le cadre du traitement des données à caractère personnel. Ainsi, l'hébergeur ne doit pas faire appel à un sous-traitant sans l'information préalable du client.	oui		Est appliqué
HDS 4.4.5. Responsabilité					
4.4.5.1.	Notification en cas d'atteinte à la sécurité des données	L'hébergeur notifie son client de toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.	oui		Est appliqué
4.4.5.2.	Période de conservation des politiques de sécurité	Les durées de rétention des différentes versions du corpus documentaire sécurité doivent être définies et formalisées.	oui		Est appliqué
4.4.5.3.	Gestion des informations personnelles: exigence principalle	L'hébergeur doit avoir défini et formalisé une politique encadrant la mise à disposition et la restitution des données à caractère personnel à ses clients, ainsi que leur destruction. Cette politique doit être communiquée au client sur demande.	oui		Est appliqué
4.4.5.3.	Gestion des informations personnelles: exigence complémentaire	Une procédure de réversibilité définissant les modalités de restitution des données en fin de contrat ou retrait de la certification doit être formalisée et appliquée	oui		Est appliqué
HDS 4.4.6. Sécurité des données					

4.4.6.1.	Les accords de confidentialité ou de non-divulgation	Les contrats de travail des salariés de l'hébergeur doivent inclure une clause de confidentialité. En cas de recours à la sous-traitance, cette exigence s'applique également aux prestataires.	oui		Est appliqué
4.4.6.2.	Restriction sur l'usage de copies papier	L'hébergeur doit restreindre le recours à des copies papier.	oui		Est appliqué
4.4.6.3.	Contrôle et traçabilité lors de la restauration de données	L'hébergeur doit disposer d'une procédure encadrant la restauration des données. Les opérations de restauration effectuées doivent être journalisées.	oui		Est appliqué
4.4.6.4.	Protection des données présentes sur un support de stockage en dehors du lieu d'hébergement	Si des supports de stockage portables contenant des données à caractère personnel sont sortis des locaux de l'hébergeur, une autorisation préalable devra être obtenue. Ces données ne doivent pas être accessibles à du personnel non autorisé, par exemple en les protégeant par des solutions de chiffrement à l'état de l'art.	oui		Est appliqué
4.4.6.5.	Utilisation de support de stockage portable	L'utilisation de supports de stockage portables incompatibles avec des solutions de chiffrement doit être proscrite.	oui		Est appliqué
4.4.6.6.	Chiffrement des données personnelles transmises sur des réseaux publics	Les données à caractère personnel doivent être chiffrées avant d'être transmises sur des réseaux publics.	oui		Est appliqué
4.4.6.7.	Destruction des copies papier	La destruction des copies papier doit être effectuée avec des moyens appropriés	oui		Est appliqué
4.4.6.8.1	Utilisation d'identifiants uniques: exigence principale	L'accès aux données à caractère personnel ou aux systèmes utilisés pour leur traitement doit être réalisé à l'aide de comptes nominatifs.	oui		Est appliqué
4.4.6.8.2	Utilisation d'identifiants uniques: exigence complémentaire	Des moyens de traçabilité doivent être mis en œuvre afin de contrôler les actions et les usages des identifiants génériques. Méthode de contrôle : l'organisme de certification doit : • s'assurer que la politique de gestion des comptes génériques limite leur usage à des cas particuliers et identifiés, par exemple en raison de contraintes intrinsèques de certains équipements ou logiciels ; • s'assurer que les traces nominatives et horodatées d'utilisation des comptes génériques sont incluses dans la politique de gestion des traces.	oui		Est appliqué
4.4.6.9.	Gestion des habilitations	Un processus de gestion des habilitations doit être défini et appliqué avec notamment la tenue d'un registre actualisé des utilisateurs ou profils utilisateurs ayant accès aux données à caractère personnel ou aux systèmes utilisés pour leur traitement.	oui		Est appliqué

4.4.6.10.1	Gestion des traces: exigence principale	L'hébergeur doit mettre en œuvre les moyens d'assurer la traçabilité des actions des utilisateurs, des défaillances et des événements liés à la sécurité de l'information. Les journaux contenant les traces doivent être conservés et revus régulièrement. L'hébergeur doit assurer l'intégrité des journaux et les protéger des accès illicites. En complément, les activités des administrateurs système et des opérateurs techniques doivent être tracées ; les journaux associés doivent être protégés et revus régulièrement. Afin de garantir la fiabilité des journaux, l'hébergeur doit s'assurer de la synchronisation de l'ensemble des horloges des systèmes (référence temporelle unique).	oui		Est appliqué
4.4.6.10.2	Gestion des traces: exigence complémentaire	Des moyens techniques et organisationnels doivent être mis en œuvre afin de communiquer au client les traces des administrateurs. Méthode de contrôle : s'assurer que l'hébergeur a formalisé et mis en œuvre les moyens organisationnels et techniques permettant de traiter les demandes de ses clients relatives aux traces d'accès des administrateurs de l'hébergeur aux systèmes d'information de santé hébergés.	oui		Est appliqué
4.4.6.11.	Gestion des identifiants	Les comptes désactivés ou expirés ne doivent pas être réattribués à de nouvelles personnes.	oui		Est appliqué
4.4.6.12.	Clauses contractuelles	Les contrats passés entre l'hébergeur et ses clients doivent spécifier les mesures techniques et organisationnelles prévues pour répondre aux objectifs de sécurité et de protection des données à caractère personnel, ainsi que les finalités de traitement. Des changements dans ces mesures ne doivent pas aboutir à une réduction du niveau de sécurité, sauf accord préalable du client.	oui		Est appliqué
4.4.6.13.	Sous-traitance du traitement des données personnelles	En cas de recours par l'hébergeur à la sous-traitance, le contrat afférent doit spécifier les mesures techniques et organisationnelles prévues pour répondre aux objectifs de sécurité et de protection des données à caractère personnel. Des changements dans ces mesures ne doivent pas aboutir à une réduction du niveau de sécurité, sauf accord préalable de l'hébergeur. L'hébergeur doit s'assurer que ce niveau de sécurité respecte les engagements pris avec ses clients.	oui		Est appliqué
4.4.6.14.	Réutilisation des espaces de stockage	L'hébergeur doit s'assurer qu'en cas de réaffectation d'espaces de stockage, ceux-ci ont bien été préalablement purgés et qu'aucune ancienne donnée ne peut être accédée.	oui		Est appliqué
HDS 4.4.7.	Localisation des données				

4.4.7.1.1	Lieux d'hébergement: exigence principale	L'hébergeur doit spécifier la liste de l'ensemble des pays au sein desquels les données du client sont ou peuvent être hébergées.	oui		Est appliqué
4.4.7.1.2	Lieux d'hébergement: exigence complémentaire	L'hébergeur doit informer son client des lieux d'hébergement et lui permettre de choisir le(s) pays d'hébergement dans le(s)quel(s) les données de santé seront hébergées et mettre en œuvre les mesures permettant de respecter ce choix.	oui		Est appliqué
HDS 4.5.Exigences complémentaires					
4.5.1.	Rôles et responsabilités	La répartition des responsabilités en termes de sécurité de l'information entre l'hébergeur et son client doit être définie et formalisée.	oui		Est appliqué
4.5.2.	Conformité aux référentiels opposables de la PGSSI-S	L'hébergeur doit informer ses clients qu'ils sont tenus de respecter la PGSSI-S (politique générale de sécurité des systèmes d'information de santé) et doit mettre en place un moyen de recueillir l'engagement de ce respect. Méthode de contrôle : • L'hébergeur doit informer ses clients qu'ils sont tenus de mettre en œuvre un système d'information de santé respectant la PGSSI-S ; • L'hébergeur doit définir et mettre en place un moyen de recueillir l'engagement de ses clients de respecter les référentiels opposables de la PGSSI-S. Cet engagement pourrait être encadré dans le contrat d'hébergement.	oui		Est appliqué
4.5.3.	Rapports d'audit	L'hébergeur doit communiquer les rapports d'audit de certification aux clients qui en font la demande. Il doit également fournir ces rapports à l'organisme de certification, en cas de transfert ou de demande d'équivalence.	oui		Est appliqué

4.5.4.	Liste des contacts clients	L'hébergeur doit maintenir une liste des points de contact pour chacun des clients. Ce point de contact doit être en mesure de désigner à l'hébergeur un professionnel de santé lorsque cela est nécessaire (exemples : accès aux données de santé, gestion des relations avec le patient, etc.) L'hébergeur doit être en capacité de transmettre sans délai cette liste à l'autorité compétente sur demande, notamment en cas de suspension ou de retrait de la certification. Méthode de contrôle : • Vérifier que la liste de contacts des clients de l'hébergeur contient, a minima, les informations suivantes : o La raison sociale du client ; o Les nom et prénom du contact ; o L'adresse mail du contact ; o Le numéro de téléphone du contact ; • Vérifier que cette liste est mise à jour régulièrement.	oui		Est appliqué
4.5.5.	Régionalisation	Régionalisation des relations avec le client. Méthode de contrôle : • S'assurer que les interfaces proposées aux clients sont disponibles au moins en langue française. • L'hébergeur doit assurer un support de premier niveau au moins en langue française. • Vérifier que la DdA est disponible au moins en langue française.	oui		Est appliqué