Déclaration d’applicabilité v24 simplifié

La présente Déclaration d’Applicabilité constitue une version simplifiée de la Déclaration d’Applicabilité complète (version 24), associée au certificat ISO/IEC 27001:2022 de la société Siagilus. Elle est destinée à être communiquée aux parties intéressées internes et externes du SMSI de Siagilus.

Les mesures de sécurité de l’information sont issues de l’annexe A de la norme ISO/IEC 27001:2022.

Mesures de sécurités de l’information	**Description**	**Applicable** (Oui/Non)
5.1 Politiques de sécurité de l'information	Une politique de sécurité de l'information et des politiques spécifiques à une thématique doivent être définies, approuvées par la direction, publiées, communiquées et demandée en confirmation au personnel et aux parties intéressées concernés, ainsi que révisées à intervalles planifiés et si des changements significatifs ont lieu.	OUI
5.2 Fonctions et responsabilités liées à la sécurité de l'information	Les fonctions et responsabilités liées à la sécurité de l'information doivent être définies et attribuées selon les besoins de l'organisation.	OUI
5.3 Séparation des tâches	Les tâches et les domaines de responsabilité incompatibles doivent être séparés.	OUi
5.4 Responsabilités de la direction	La direction doit demander à tout le personnel d'appliquer les mesures de sécurité de l'information conformément à la politique de sécurité de l'information, aux politiques spécifiques à une thématique et aux procédures établies de l'organisation.	OUI
5.5 Contacts avec les autorités	L'organisation doit établir et maintenir le contact avec les autorités appropriées.	OUI

5.6 Contacts avec des groupes d'intérêt spécifiques	L'organisation doit établir et maintenir des contacts avec des groupes d'intérêt spécifiques ou autres forums spécialisés sur la sécurité et associations professionnelles.	OUI
5.7 Renseignement sur les menaces	Les informations relatives aux menaces de sécurité de l'information doivent être collectées et analysées pour produire les renseignements sur les menaces.	OUI
5.8 Sécurité de l'information dans la gestion de projet	La sécurité de l'information doit être intégrée à la gestion de projet.	OUI
5.9 Inventaire des informations et autres actifs associés	Un inventaire des informations et des autres actifs associés, y compris leurs propriétaires, doit être élaboré et tenu à jour.	OUI
5.10 Utilisation correcte des informations et autres actifs associés	Des règles d'utilisation correcte et des procédures de traitement des informations et autres actifs associés doivent être identifiées, documentées et mises en oeuvre.	OUI
5.11 Restitution des actifs	Le personnel et les autres parties intéressées, selon le cas, doivent restituer tous les actifs de l'organisation qui sont en leur possession au moment du changement ou de la fin de leur emploi, contrat ou accord.	OUI
5.12 Classification des informations	Les informations doivent être classifiées conformément aux besoins de sécurité de l'information de l'organisation, sur la base des exigences de confidentialité, d'intégrité, de disponibilité, et des exigences importantes des parties intéressées.	OUI
5.13 Marquage des informations	Un ensemble approprié de procédures pour le marquage des informations doit être élaboré et mis en oeuvre conformément au schéma de classification des informations adopté par l'organisation.	OUI
5.14 Transfert des informations	Des règles, procédures ou accords sur le transfert des informations doivent être mis en place pour tous les	OUI

	types de moyens de transfert au sein de l'organisation et entre l'organisation et des tierces parties.	
5.15 Contrôle d'accès	Des règles visant à contrôler l'accès physiques et logique aux informations et autres actifs associés doivent être définies et mises en oeuvre, en fonction des exigences métier et de sécurité de l'information.	OUI
5.16 Gestion des identités	Le cycle de vie complet des identités doit être géré.	OUI
5.17 Informations d'authentification	L'attribution et la gestion des informations d'authentification doivent être contrôlées par un processus de gestion, incluant des recommandations au personnel sur l'utilisation appropriée des informations d'authentification.	OUI
5.18 Droits d'accès	Les droits d'accès aux informations et autres actifs associés doivent être pourvus, révisés, modifiés et supprimés conformément à la politique spécifique à la thématique du contrôle d'accès et aux règles de contrôle d'accès de l'organisation.	OUI
5.19 Sécurité de l'information dans les relations avec les fournisseurs	Des processus et procédures pour gérer les risques de sécurité de l'information qui sont associés à l'utilisation des produits ou services du fournisseur doivent être définis et mis en oeuvre.	OUI
5.20 La sécurité de l'information dans les accords conclus avec les fournisseurs	Les exigences de sécurité de l'information appropriées doivent être mises en place et convenues avec chaque fournisseur, selon le type de relation avec le fournisseur.	OUI
5.21 Gestion de la sécurité de l'information dans la chaîne d'approvisionnement des technologies de l'information et de la communication (TIC)	Des processus et procédures pour gérer les risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et services TIC doivent être définis et mis en oeuvre.	OUI

5.22 Surveillance, révision et gestion des changements des services fournisseurs	L'organisation doit procéder régulièrement à la surveillance, à la révision, à l'évaluation et à la gestion des changements des pratiques de sécurité de l'information du fournisseur et de prestation de services.	OUI
5.23 Sécurité de l'information dans l'utilisation de services en nuage	Les processus d'acquisition, d'utilisation, de gestion et de cessation des services en nuage doivent être établis conformément aux exigences de sécurité de l'information de l'organisation.	OUI
5.24 Planification et préparation de la gestion des incidents de sécurité de l'information	L'organisation doit planifier et préparer la gestion des incidents de sécurité de l'information en procédant à la définition, à l'établissement et à la communication des processus, fonctions et responsabilités liés à la gestion des incidents de sécurité de l'information.	OUI
5.25 Évaluation des événements de sécurité de l'information et prise de décision	L'organisation doit évaluer les événements de sécurité de l'information et décider s'ils doivent être catégorisés comme des incidents de sécurité de l'information.	OUI
5.26 Réponse aux incidents de sécurité de l'information	La réponse aux incidents de sécurité de l'information doit être conforme aux procédures documentées.	OUI
5.27 Tirer des enseignements des incidents de sécurité de l'information	Les connaissances acquises à partir des incidents de sécurité de l'information doivent être utilisées pour renforcer et améliorer les mesures de sécurité de l'information.	OUI
5.28 Collecte de preuves	L'organisation doit établir et mettre en oeuvre des procédures pour l'identification, la collecte, l'acquisition et la préservation des preuves relatives aux événements de sécurité de l'information.	OUI
5.29 Sécurité de l'information pendant une perturbation	L'organisation doit planifier comment maintenir la sécurité de l'information au niveau approprié pendant une perturbation.	OUI

5.30 Préparation des TIC pour la continuité d'activité	La préparation des TIC doit être planifiée, mise en oeuvre, maintenue et testée en se basant sur les objectifs de continuité d'activité et des exigences de continuité des TIC.	OUI
5.31 Exigences légales, statutaires, réglementaires et contractuelles	Les exigences légales, statutaires, réglementaires et contractuelles pertinentes pour la sécurité de l'information, ainsi que l'approche de l'organisation pour respecter ces exigences, doivent être identifiées, documentées et tenues à jour.	OUI
5.32 Droits de propriété intellectuelle	L'organisation doit mettre en oeuvre les procédures appropriées pour protéger les droits de propriété intellectuelle.	OUI
5.33 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.	OUI
5.34 Protection de la vie privée et des données à caractère personnel (DCP)	L'organisation doit identifier et respecter les exigences relatives à la protection de la vie privée et des DCP conformément aux lois, réglementations et exigences contractuelles applicables.	OUI
5.35 Révision indépendante de la sécurité de l'information	L'approche de l'organisation pour gérer la sécurité de l'information et sa mise en oeuvre, y compris les personnes, les processus et les technologies, doit être révisée de manière indépendante à intervalles planifiés, ou lorsque des changements significatifs se produisent.	OUI
5.36 Conformité aux politiques, règles et normes de sécurité de l'information	La conformité à la politique de sécurité de l'information, aux politiques spécifiques à une thématique, aux règles et aux normes de l'organisation doit être régulièrement vérifiée.	OUI
5.37 Procédures d'exploitation documentées	Les procédures d'exploitation des moyens de traitement de l'information doivent être documentées et mises à disposition du personnel qui en a besoin.	OUI
6.1 Sélection des candidats	Les vérifications des références de tous les candidats à l'embauche doivent être réalisées avant qu'ils n'intègrent	OUI

	l'organisation puis de façon continue en tenant compte des lois, des réglementations et de l'éthique applicables, et doivent être proportionnelles aux exigences métier, à la classification des informations auxquelles ils auront accès et aux risques identifiés.	
6.2 Termes et conditions du contrat de travail	Les contrats de travail doivent indiquer les responsabilités du personnel et de l'organisation en matière de sécurité de l'information.	OUI
6.3 Sensibilisation, enseignement et formation en sécurité de l'information	Le personnel de l'organisation et les parties intéressées pertinentes doivent recevoir une sensibilisation, un enseignement et des formations en sécurité de l'information appropriés, ainsi que des mises à jour régulières de la politique de sécurité de l'information, des politiques spécifiques à une thématique et des procédures de l'organisation pertinentes à leur fonction.	OUI
6.4 Processus disciplinaire	Un processus disciplinaire permettant de prendre des mesures à l'encontre du personnel et d'autres parties intéressées qui ont commis une violation de la politique de sécurité de l'information doit être formalisé et communiqué.	OUI
6.5 Responsabilités après la fin ou le changement d'un emploi	Les responsabilités et les obligations relatives à la sécurité de l'information qui restent valables après la fin ou le changement d'un emploi doivent être définies, appliquées et communiquées au personnel et autres parties intéressées pertinentes.	OUI
6.6 Accords de confidentialité ou de non-divulgation	Des accords de confidentialité ou de non-divulgation, représentant les besoins de l'organisation relatifs à la protection des informations, doivent être identifiés, documentés, régulièrement révisés et signés.	OUI
6.7 Travail à distance	Des mesures de sécurité doivent être mises en oeuvre lorsque le personnel travaille à distance, pour protéger les informations accessibles, traitées ou stockées en dehors des locaux de l'organisation.	OUI

6.8 Déclaration des événements de sécurité de l'information	L'organisation doit fournir un mécanisme au personnel pour déclarer rapidement les événements de sécurité de l'information observés ou suspectés, à travers des canaux appropriés.	OUI
7.1 Périmètres de sécurité physique	Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones qui contiennent les informations et autres actifs associés.	OUI
7.2 Les entrées physiques	Les zones sécurisées doivent être protégées par des mesures de sécurité des accès et des points d'accès appropriés.	OUI
7.3 Sécurisation des bureaux, des salles et des installations	Des mesures de sécurité physique pour les bureaux, les salles et les installations doivent être conçues et mises en oeuvre.	OUI
7.4 Surveillance de la sécurité physique	Les locaux doivent être continuellement surveillés pour empêcher l'accès physique non autorisé.	OUI
7.5 Protection contre les menaces physiques et environnementales	Une protection contre les menaces physiques et environnementales, telles que les catastrophes naturelles et autres menaces physiques, intentionnelles ou non intentionnelles, impactant l'infrastructure, doit être conçue et mise en œuvre.	OUI
7.6 Travail dans les zones sécurisées	Des mesures de sécurité pour le travail dans les zones sécurisées doivent être conçues et mises en œuvre.	Oui
7.7 Bureau propre et écran vide	Des règles du bureau vide, dégagé des documents papier et des supports de stockage amovibles, et des règles de l'écran vide pour les moyens de traitement de l'information, doivent être définies et appliquées de manière appropriée.	OUI
7.8 Emplacement et protection du matériel	Un emplacement sécurisé pour le matériel doit être choisi et protégé.	OUI
7.9 Sécurité des actifs hors des locaux	Les actifs hors du site doivent être protégés.	OUI

7.10 Supports de stockage	Les supports de stockage doivent être gérés tout au long de leur cycle de vie d'acquisition, d'utilisation, de transport et de mise au rebut, conformément au schéma de classification et aux exigences de traitement de l'organisation.	OUI
7.11 Services supports	Les moyens de traitement de l'information doivent être protégés contre les coupures de courant et autres perturbations causées par des défaillances des services supports.	OUI
7.12 Sécurité du câblage	Les câbles électriques, transportant des données ou supportant les services d'information, doivent être protégés contre des interceptions, interférences ou dommages.	OUI
7.13 Maintenance du matériel	Le matériel doit être entretenu correctement pour assurer la disponibilité, l'intégrité et la confidentialité de l'information.	OUI
7.14 Élimination ou recyclage sécurisé(e) du matériel	Les éléments du matériel contenant des supports de stockage doivent être vérifiés pour s'assurer que toute donnée sensible et que tout logiciel sous licence ont été supprimés ou écrasés de façon sécurisée, avant son élimination ou sa réutilisation.	OUI
8.1 Terminaux finaux des utilisateurs	Les informations stockées, traitées ou accessibles via les terminaux finaux des utilisateurs, doivent être protégées.	OUI
8.2 Droits d'accès privilégiés	L'attribution et l'utilisation des droits d'accès privilégiés doivent être limitées et gérées.	OUI
8.3 Restriction d'accès aux informations	L'accès aux informations et autres actifs associés doit être restreint conformément à la politique spécifique à la thématique du contrôle d'accès qui a été établie.	OUI
8.4 Accès aux codes source	L'accès en lecture et en écriture au code source, aux outils de développement et aux bibliothèques de logiciels doit être géré de manière appropriée.	OUI

8.5 Authentification sécurisée	Des technologies et procédures d'authentification sécurisées doivent être mises en œuvre sur la base des restrictions d'accès aux informations et de la politique spécifique à la thématique du contrôle d'accès.	OUI
8.6 Dimensionnement	L'utilisation des ressources doit être surveillée et ajustée selon les besoins de dimensionnement actuels et prévus.	OUI
8.7 Protection contre les programmes malveillants (malware)	Une protection contre les programmes malveillants doit être mise en œuvre et renforcée par une sensibilisation appropriée des utilisateurs.	OUI
8.8 Gestion des vulnérabilités techniques	Des informations sur les vulnérabilités techniques des systèmes d'information utilisés doivent être obtenues, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et des mesures appropriées doivent être prises.	OUI
8.9 Gestion des configurations	Les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux, doivent être définies, documentées, mises en œuvre, surveillées et révisées.	OUI
8.10 Suppression des informations	Les informations stockées dans les systèmes d'information, les terminaux ou tout autre support de stockage doivent être supprimées lorsqu'elles ne sont plus nécessaires.	OUI
8.11 Masquage des données	Le masquage des données doit être utilisé conformément à la politique spécifique à la thématique du contrôle d'accès de l'organisation et d'autres politiques spécifiques à une thématique associées, ainsi qu'aux exigences métier, tout en prenant en compte la législation applicable.	OUI
8.12 Prévention de la fuite de données	Des mesures de prévention de la fuite de données doivent être appliquées aux systèmes, aux réseaux et à tous les autres terminaux qui traitent, stockent ou transmettent des informations sensibles.	OUI

8.13 Sauvegarde des informations	Des copies de sauvegarde de l'information, des logiciels et des systèmes doivent être conservées et testées régulièrement selon la politique spécifique à la thématique de la sauvegarde qui a été convenue.	OUI
8.14 Redondance 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
8.15 Journalisation	Des journaux qui enregistrent les activités, les exceptions, les pannes et autres événements pertinents doivent être générés, conservés, protégés et analysés.	OUI
8.16 Activités de surveillance	Les réseaux, systèmes et applications doivent être surveillés pour détecter les comportements anormaux et des mesures appropriées doivent être prises pour évaluer les éventuels incidents de sécurité de l'information.	OUI
8.17 Synchronisation des horloges	Les horloges des systèmes de traitement de l'information utilisés par l'organisation doivent être synchronisées avec des sources de temps approuvées.	OUI
8.18 Utilisation de programmes utilitaires à privilèges	L'utilisation des programmes utilitaires ayant la capacité de contourner les mesures de sécurité des systèmes ou des applications doit être limitée et contrôlée étroitement.	OUI
8.19 Installation de logiciels sur des systèmes opérationnels	Des procédures et des mesures doivent être mises en oeuvre pour gérer de manière sécurisée l'installation de logiciels sur les systèmes opérationnels.	OUI
8.20 Sécurité des réseaux	Les réseaux et les terminaux réseau doivent être sécurisés, gérés et contrôlés pour protéger les informations des systèmes et des applications.	OUI
8.21 Sécurité des services réseau	Les mécanismes de sécurité, les niveaux de service et les exigences de services des services réseau doivent être identifiés, mis en oeuvre et surveillés.	OUI

8.22 Cloisonnement des réseaux	Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés dans les réseaux de l'organisation.	OUI
8.23 Filtrage web	L'accès aux sites web externes doit être géré pour réduire l'exposition aux contenus malveillants.	OUI
8.24 Utilisation de la cryptographie	Des règles pour l'utilisation efficace de la cryptographie, notamment la gestion des clés cryptographiques, doivent être définies et mises en œuvre.	OUI
8.25 Cycle de vie de développement sécurisé	Des règles pour le développement sécurisé des logiciels et des systèmes doivent être définies et appliquées.	OUI
8.26 Exigences de sécurité des applications	Les exigences de sécurité de l'information doivent être identifiées, spécifiées et approuvées lors du développement ou de l'acquisition d'applications.	OUI
8.27 Principes d'ingénierie et d'architecture des systèmes sécurisés	Des principes d'ingénierie des systèmes sécurisés doivent être établis, documentés, tenus à jour et appliqués à toutes les activités de développement de systèmes d'information.	OUI
8.28 Codage sécurisé	Des principes de codage sécurisé doivent être appliqués au développement de logiciels.	OUI
8.29 Tests de sécurité dans le développement et l'acceptation	Des processus pour les tests de sécurité doivent être définis et mis en oeuvre au cours du cycle de vie de développement.	OUI
8.30 Développement externalisé	L'organisation doit diriger, contrôler et vérifier les activités relatives au développement externalisé des systèmes.	NON
8.31 Séparation des environnements de développement, de test et opérationnels	Les environnements de développement, de test et opérationnels doivent être séparés et sécurisés.	OUI
8.32 Gestion des changements	Les changements apportés aux moyens de traitement de l'information et aux systèmes d'information doivent être	OUI

	soumis à des procédures de gestion des changements.	
8.33 Informations de test	Les informations de test doivent être sélectionnées, protégées et gérées de manière appropriée.	OUI
8.34 Protection des systèmes d'information pendant les tests d'audit	Les tests d'audit et autres activités d'assurance impliquant l'évaluation des systèmes opérationnels doivent être planifiés et convenus entre le testeur et le niveau approprié de la direction.	OUI