ANNEXE 2 - SYSTÈME DE CLASSE I - EXIGENCES DE SÉCURITÉ DE L'UNICEF

1. Catégorisation

Ce document décrit les exigences de sécurité de l'UNICEF pour les systèmes classifiés comme étant de Classe I. L'UNICEF reconnaît 4 classes d'information : Classe I - Confidentielle, Classe II - Interne, Classe III - Restreinte et Classe VI - Publique. Toutes les classes sont basées sur la valeur métier de l'information. Les systèmes de Classe I portent la classification la plus élevée de toute l'organisation. Cette classification est désignée pour les actifs TIC (Technologies de l'Information et de la Communication) de l'UNICEF hautement sensibles et critiques.

Classification du Système	Description	Confidentialité	Intégrité	Disponibilité
Classe I	Un système qui stocke et/ou traite des informations confidentielles critiques pour les opérations de l'UNICEF, la sécurité des individus et/ou est directement lié à des processus métier critiques. Un accès non autorisé peut gravement impacter les opérations/processus métier de l'UNICEF, la sécurité personnelle des individus et/ou leur identité.	**ÉLEVÉE**	**ÉLEVÉE**	**ÉLEVÉE**

2. Applicabilité / Portée

Les exigences de sécurité décrites dans ce document sont obligatoires et s'appliquent à toute partie interne ou externe qui fournit une solution, un système ou un service à l'UNICEF qui traite, stocke ou transmet des informations répondant aux critères de classification reflétés dans ce document.

2.1. Propriétés d'un Système de Classe I

La propriété déterminante d'un système de Classe I est la suivante : un système/service qui traite et/ou stocke des données personnelles ou des données confidentielles de l'UNICEF ou qui est lié à un ou plusieurs processus métier critiques, tels que définis dans cette section.

Données personnelles

L'UNICEF définit les données personnelles de manière similaire à l'article 9 du Règlement Général sur la Protection des Données 2016/679 (RGPD) de l'UE :

« Données concernant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».

« Données de profilage, lorsqu'il s'agit de toute forme de traitement automatisé de données à caractère personnel consistant à utiliser des données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. »

Tout système qui traite et/ou stocke des données personnelles est un système de Classe I.

Données confidentielles de l'UNICEF

Informations telles que, mais sans s'y limiter, les rapports sensibles de la Division des Programmes, les dossiers des Ressources Humaines, les documents d'enquête, etc. Tout système qui traite et/ou stocke des données confidentielles de l'UNICEF est un système de Classe I.

3. Exigences de Sécurité

Toutes les exigences couvertes dans cette section reflètent des contrôles qui doivent être inclus dans toute Demande de Proposition (RFP), bon de commande / Termes de Référence (ToR) ou tout document pouvant être utilisé par un fournisseur de services ou une entité de services professionnels qui fournit au ministère de la santé un "Produit" ou un "Service".
Le responsable métier (responsable du traitement des données) et Le prestataire de services(sous-traitant) tous deux partagent l'obligation de garantir la bonne mise en œuvre de ces exigences.
Il convient de noter que les exigences décrites dans cette section doivent être considérées comme une couche supplémentaire pour compléter l'écosystème de sécurité existant des fournisseurs et non comme un remplacement. Dans les cas où les contrôles d'un fournisseur de services sont plus restrictifs, les contrôles du fournisseur de services prévaudront et seront formellement consignés par les deux parties.

3.1. Exigences Générales de Sécurité

a) Le ministère de la santé se réserve le droit d'évaluer la qualité et l'exactitude du développement logiciel externalisé et de la maintenance opérationnelle du système/application, que ce soit par des tests d'assurance sécurité ou par une évaluation de sécurité externe.
b) La solution/le service doit être protégé du trafic réseau indésirable par des mesures de filtrage ou de séparation du réseau qui se situent en dehors du système, telles que des routeurs et des pare-feu contrôlés de l'extérieur.
c) Le système doit disposer d'une protection adéquate des terminaux (end-point), avec les exigences minimales suivantes :
* Mesures de protection contre les codes malveillants.
* Pare-feu hôte configuré en utilisant, au minimum, les contrôles d'accès du moindre privilège (services, utilisateurs, accès à la communication).

3.2. Validation des Contrôles de Sécurité

a) Le ministère de la santé se réserve le droit de valider périodiquement la mise en œuvre des exigences de sécurité décrites dans ce document via :
* Tests d'Assurance Sécurité
* Tests de Vulnérabilité
* Tests d'Intrusion (Penetration Testing)
* Audits
* Contrôles sur site

3.3. Conformité & Certifications

a) Tout fournisseur qui héberge un système de classe I doit détenir, au minimum, une certification ISO 2700K et fournir les documents suivants pour consultation : Certification ISO, Déclaration d'Applicabilité (SoA), rapports d'audit SOC 2 et SOC 3.

3.4. Identification, Authentification et Autorisation

a) Le prestataire de services doit suivre le principe du moindre privilège, garantissant que les identifiants d'utilisateurs, de groupes, de rôles et d'appareils seront uniques et attribués à chaque entité (utilisateur ou processus). Chaque rôle d'utilisateur de l'application doit avoir une connexion à la base de données correspondante selon ses privilèges.
b) Le prestataire de services doit gérer de manière centralisée les comptes utilisateurs en utilisant des identités fédérées et, lorsque cela est possible, intégrer sa solution au système de gestion des identités du ministère de la santé.
* Si l'authentification est basée sur un mot de passe, celui-ci doit obligatoirement respecter les exigences de qualité des meilleures pratiques courantes et être renouvelé de force fréquemment. L'attribution des authentifiant sera contrôlée et gérée par un processus formel.
c) L'authentification multi-facteurs sera utilisée pour :
* les comptes à privilèges et
* l'accès des utilisateurs en dehors du réseau de confiance du ministère de la santé.
d) Tous les comptes utilisateurs et système doivent être désactivés après une période d'inactivité définie, conformément aux normes de l'organisation. Tous les comptes et/ou mots de passe par défaut doivent être supprimés ou modifiés.
Des approbations seront requises pour la création, la suppression ou la modification de tout compte.
e) Tout accès depuis des réseaux externes doit passer par des points d'entrée et de sortie spécifiques où la

communication externe est terminée et rétablie dans un écosystème IT contrôlé par le ministère de la santé.
f) Des fonctionnalités de verrouillage de compte seront utilisées en cas de tentatives d'authentification invalides.
g) Le code de l'application ne doit jamais contenir d'informations d'identification.

3.5. Disponibilité et Suppression

a) La disponibilité des systèmes doit être définie conformément aux Accords de Niveau de Service (SLA), pour répondre aux exigences de Confidentialité, d'Intégrité et de Disponibilité proportionnelles à sa classification, comme indiqué ci-dessus.
b) Toute suppression de données confidentielles/personnelles doit être effectuée de manière à ce qu'elles ne puissent pas être reconstituées.

3.6. Cryptographie

a) Le système doit disposer de contrôles cryptographiques pour sécuriser les données sensibles en transit, au repos et en cours d'utilisation. Au minimum, les normes cryptographiques du ministère de la santé doivent être utilisées. Dans les cas où les normes cryptographiques du fournisseur dépassent les normes organisationnelles publiées, les contrôles techniques du fournisseur prévaudront.
b) Les données personnelles doivent être masquées, anonymisées ou autrement protégées contre tout accès non autorisé.
c) Le prestataire de services doit utiliser les meilleures pratiques ou les protocoles d'échange de données sécurisés standards de l'industrie et les maintenir à jour, conformément aux normes définies par le ministère de la santé. Les protocoles obsolètes et/ou compromis ne doivent jamais être utilisés.
d) Tous les mots de passe doivent être chiffrés avec les meilleures pratiques actuelles ou des algorithmes cryptographiques et des clés sécurisées standards de l'industrie. Les clés seront générées à l'aide d'algorithmes cryptographiques forts.
e) Les fichiers de clés doivent être protégés contre toute modification non autorisée à l'aide d'une application qui applique une réconciliation automatique à partir d'une source faisant autorité.
f) Les clés de chiffrement doivent être stockées de manière sécurisée en dehors des systèmes sur lesquels elles sont utilisées.

3.7. Développement Sécurisé

a) Le système doit être conçu en suivant les principes de "sécurité dès la conception" (security by design)[1].
b) Le système doit être développé en suivant le principe de "protection des données dès la conception et par défaut"[2]. Par conséquent, des mesures techniques et organisationnelles appropriées doivent être en place pour mettre en œuvre les principes de protection des données et garantir les droits individuels. La protection des données doit être intégrée dans les activités de traitement et les pratiques opérationnelles, depuis la phase de conception et tout au long du cycle de vie de la solution.
c) Le développement et les tests du système seront effectués avec des informations fictives ou anonymisées.
d) Tout code source développé spécifiquement pour le système doit faire l'objet d'un test d'assurance sécurité et d'une analyse d'impact sur les activités pour ramener le risque opérationnel à un niveau acceptable. Le niveau de tolérance au risque doit être établi par le propriétaire du système/de la solution.
e) L'accès au code source du programme et aux éléments associés - tels que les conceptions, les spécifications, les plans de test et de validation - doit être strictement contrôlé pour empêcher l'introduction de fonctionnalités non autorisées.
f) Le système doit afficher des messages d'erreur génériques qui ne divulguent pas d'informations détaillées telles que les journaux de processus, les informations de compte ou de système.
g) Le code exécutable ne sera pas mis en œuvre sur un système opérationnel tant que la preuve de conformité aux critères de test (approbation de l'utilisateur, assurance qualité, ou l'équivalent) n'est pas acquise et que les bibliothèques de code source associées n'ont pas été mises à jour.

3.8. Mise à jour de l'inventaire des actifs

a) L'inventaire des actifs liés aux applications du ministère de la Santé doit être mis à jour, dans le cadre du processus opérationnel, en répertoriant tous les éléments du système, en décrivant leur fonction métier, leur emplacement/identifiants et leur responsable métier.

---

[1] Tel que décrit par l'OWASP sur https://www.owasp.org/index.php/Security_by_Design_Principles

[2] Tel que décrit à l'article 25 du Règlement Général sur la Protection des Données 2016/679 (RGPD) de l'UE

3.9. Opérations de Sécurité

a) Le système doit être "durci" (hardened), ce qui signifie que :
* Seuls les services et les ports réseaux nécessaires à un fonctionnement efficace sont actifs.
* Tout le code de l'application est corrigé (patché) et maintenu à jour.
* Limitation des comptes et suppression, modification ou désactivation des comptes et mots de passe par défaut.
Remarque : Afin d'assurer le suivi d'une méthodologie appropriée basée sur le risque, les correctifs doivent appartenir à l'une des catégories suivantes, classées par le fournisseur de l'application/du système : critique, non critique. Le SLA qui définit la fenêtre d'application des correctifs doit être formellement documenté par le prestataire.
b) Les serveurs et les applications doivent être configurés pour fonctionner avec les autorisations système minimales nécessaires. Le prestataire de services doit assurer la mise en œuvre des mesures techniques et organisationnelles appropriées.
c) Le système doit être configuré pour afficher des messages d'erreur génériques qui ne divulguent pas d'informations détaillées telles que les journaux de processus, les informations de compte ou de système.
d) L'environnement de production doit être séparé des environnements de test et de développement, de préférence sur des systèmes logiquement et physiquement différents.
e) L'environnement de développement et de test doit avoir le même niveau de correctifs que l'environnement de production.
f) L'environnement de production ne doit comporter aucun outil de développement.
g) Le code source de la configuration/application/travail personnalisé doit être protégé contre tout accès/modification non autorisé et résider dans un environnement de non-production avec une politique de sauvegarde/résilience appropriée.
h) Le système doit disposer de mesures de protection contre les codes malveillants. Les journaux générés par ces mesures doivent être surveillés.

3.10. Gestion des Vulnérabilités

a) Le prestataire de services est tenu d'effectuer des tests de sécurité. Ces tests seront effectués avant le lancement du système et périodiquement par la suite, avec une fréquence minimale d'une fois par an.
b) Le prestataire de services est tenu de rendre compte des résultats des analyses de sécurité et des mesures correctives prises. Ces rapports seront envoyés au Chef de la Sécurité Informatique du ministère de la santé ou au(x) point(s) focal(aux) concerné(s).
c) Les correctifs de sécurité critiques doivent être appliqués dans les 3 jours, en suivant les processus établis de test et de gestion du changement.

3.11. Gestion du Changement

a) Tout changement apporté au(x) système(s) ou logiciel(s) du ministère de la santé doit faire l'objet d'un accord entre les responsables IT, le responsable métier de la division concerné et le tiers.
b) Les changements apportés au système et/ou à l'application après la configuration de base seront documentés (numéro de version/build), avec une description via un processus formel de gestion du changement. Le prestataire de services doit rapporter, au minimum, les informations suivantes sur les correctifs : type, version, raison, résultats des tests post-implémentation. Les correctifs qui échouent aux tests seront également enregistrés et documentés.
c) La mise à jour des logiciels opérationnels, des applications et des bibliothèques de programmes ne sera effectuée que par des administrateurs formés et qualifiés, sur autorisation de la direction compétente.

3.12. Gestion et Surveillance des Journaux (Logs)

a) Le système doit générer et traiter des rapports d'audit couvrant toutes les actions entreprises sur les données personnelles, y compris l'accès aux données uniquement.
b) Les activités de validation de l'authentification et tous les changements d'autorisation doivent être journalisés et stockés de manière sécurisée, avec un accès limité.
c) L'accès au contenu, aux informations clés et/ou à toute modification des bibliothèques de programmes opérationnels doit être journalisé et restreint.
d) Les journaux et les événements seront générés dans un format qui peut être facilement analysé et utilisé comme entrée pour un processus de gestion de la journalisation.
e) Une vérification de l'intégrité des journaux doit être effectuée pour garantir la cohérence.
f) Le système, l'application, ainsi que les services et/ou réseaux sous-jacents, doivent être surveillés et leurs activités journalisées.

3.13. Gestion des Incidents de Sécurité

Une violation de la sécurité doit être considérée comme :

- Une défaillance des contrôles de sécurité entraînant l'accès, la destruction, la perte ou l'altération accidentels, illicites ou non autorisés de données/informations traitées/stockées sur le système.
- Une défaillance des contrôles de sécurité entraînant l'accès accidentel, illicite ou non autorisé à des ressources IT, telles que, mais sans s'y limiter, les ressources informatiques (traitement et/ou stockage/services) et les ressources de communication (infrastructure).

a) Les violations de sécurité doivent être immédiatement communiquées au point focal du ministère de la santé.

b) Une procédure de notification et d'escalade des incidents de sécurité doit être formellement documentée et contractuellement appliquée entre Le prestataire de services et le Centre des Opérations de Sécurité du ministère de la santé.