Plan de mise en œuvre des contrôles de sécurité pour l'UNICEF

1. Examen des normes et cadres pertinents

| **Norme/Cadre** | **Aperçu** | **Application** | **Avantages clés** | |---|---|---|---| | **ISO/IEC 27001 : Système de gestion de la sécurité de l'information (ISMS)** | Une norme internationale pour la mise en œuvre, l'exploitation et la maintenance d'un SMSI afin de protéger les informations sensibles. | L'UNICEF adoptera le cadre ISO/IEC 27001 pour créer un SMSI complet qui répond aux besoins de ses opérations à l'échelle mondiale, couvrant les dossiers de santé sensibles, les informations sur les donateurs et les données sur la protection de l'enfance. | Crée une culture de sécurité de l'information unifiée à l'échelle de l'organisation ; réduit le risque de violation de données et de non-conformité ; améliore la confiance des parties prenantes et l'assurance mondiale de la protection des données. | | **NIST SP 800-53 : Contrôles de sécurité et de confidentialité pour les systèmes d'information** | Un ensemble de contrôles fédéraux de sécurité et de confidentialité conçus pour protéger les données et les systèmes de l'organisation tout au long de leur cycle de vie. | L'UNICEF intégrera les contrôles NIST SP 800-53 pour sécuriser les systèmes gérant les données sensibles et garantir l'adoption des meilleures pratiques sur toutes les plateformes technologiques, de la sécurité des réseaux à la confidentialité des données. | S'aligne sur les normes du gouvernement américain, fournit des directives claires en matière de cybersécurité et intègre la protection de la vie privée aux mesures de sécurité opérationnelle. | | **Contrôles CIS (Centre pour la sécurité Internet)** | Un ensemble hiérarchisé de bonnes pratiques en matière de cybersécurité axé sur la réduction des risques liés aux cyberattaques courantes. | L'UNICEF mettra en œuvre les contrôles CIS 1 à 20, allant de l'inventaire et du contrôle du matériel et des logiciels à la réponse aux incidents et à la récupération, afin d'atténuer les cybermenaces généralisées. | Fournit un ensemble de contrôles exploitables et faciles à mettre en œuvre ; hautement évolutif pour différentes parties de l'organisation ; favorise la résilience contre les cybermenaces les plus courantes et les plus dangereuses. | | **RGPD (Règlement Général sur la Protection des Données)** | Réglementation de l'UE qui impose des contrôles stricts sur la collecte, le traitement et le stockage des données personnelles. | L'UNICEF se conformera aux réglementations RGPD dans les régions où elles sont applicables, en particulier concernant les données des résidents de l'UE, garantissant ainsi la transparence, la sécurité et la responsabilité dans le traitement des données. | Garantit le respect de la législation dans l'UE, instaure la confiance avec les donateurs et les parties prenantes et évite de lourdes amendes grâce à des pratiques strictes de protection des données. |

---

2. Contrôles de sécurité détaillés

| **Contrôle** | **Risque traité** | **Détails du contrôle** | **Normes pertinentes** | **Rôles et responsabilités** | **Chronologie** | |---|---|---|---|---|---|

----------| | **Authentification multifacteur (MFA)** | Accès non autorisé en raison d'informations d'identification compromises. | - Appliquer l'authentification multifacteur sur tous les systèmes critiques (par exemple, le système financier mondial de l'UNICEF, les portails de gestion des ressources humaines, les dossiers de protection de l'enfance).
- Facteurs requis : mot de passe + OTP (via un smartphone ou un jeton matériel).
- Méthodes de sauvegarde comme la messagerie électronique. des questions de vérification ou de sécurité seront intégrées pour la récupération. | ISO/IEC 27001 A.9.4.2, NIST 800-53 AC-2, contrôle CIS 16 | **Équipe de sécurité informatique** : Déployez et surveillez MFA.
Département RH : Garantir la conformité des employés.
Opérations de sécurité: Auditer l'efficacité de l'AMF et répondre aux problèmes. | Phase 1 : Configuration de la solution (1 mois)
Phase 2 : Déploiement MFA à l'échelle de l'organisation (2 mois)
Phase 3 : Tests et ajustements (1 mois) | | **Cryptage des données (au repos et en transit)** | Violations de données par accès non autorisé ou interception pendant la transmission/stockage. | - Toutes les données sensibles (dossiers de santé, données des donateurs, informations personnelles des employés) seront cryptées à l'aide du cryptage AES-256 (au repos) et du cryptage TLS 1.2/1.3 (en transit).
- Le système de gestion des clés (KMS) sera sécurisé gérer les clés de chiffrement tout au long de leur cycle de vie. | ISO/IEC 27001 A.10.1.1, NIST 800-53 SC-12, article 32 du RGPD | **Équipe de sécurité informatique** : Implémentez le chiffrement.
Équipes de conformité et juridiques : Assurez-vous que les méthodes de chiffrement sont conformes au RGPD.
Équipe des opérations: Auditez régulièrement l'état du chiffrement et la gestion des clés. | Phase 1 : Sélection des outils (1 mois)
Phase 2 : Déploiement (3 mois)
Phase 3 : Mise en œuvre de la gestion des clés (1 mois) | | **Pare-feu et systèmes de détection/prévention des intrusions (IDS/IPS)** | Menaces basées sur le réseau, notamment les accès non autorisés, les logiciels malveillants et les attaques DoS/DDoS. | - Déployez des pare-feu de nouvelle génération (NGFW) aux points d'entrée du réseau.
- Implémentez IDS/IPS pour détecter et prévenir les intrusions en temps réel.
- Intégrez des flux de renseignements sur les menaces pour une détection proactive des attaques. | NIST 800-53 AC-4, contrôle CIS 9, ISO/IEC 27001 A.13.1.1 | **Équipe de sécurité réseau** : Configurez les pare-feu et IDS/IPS.
SOC : Surveillez le trafic réseau et identifiez les menaces.
Administrateurs système : Assurez-vous que les pare-feu et les IPS sont configurés et testés correctement. | Phase 1 : Installation initiale (2 mois)
Phase 2 : Mises à jour régulières et optimisation des performances (En cours) | | **Contrôle d'accès basé sur les rôles (RBAC)** | Accès non autorisé en raison de l'échec de l'application du contrôle d'accès du moindre privilège. | - Mettez en œuvre RBAC pour tous les systèmes, en garantissant que les utilisateurs ont accès uniquement aux données nécessaires à leurs rôles.
- Tirez parti d'Active Directory ou de LDAP pour un contrôle d'accès centralisé.
- Audits périodiques pour garantir que l'accès reste conforme aux responsabilités professionnelles. | NIST 800-53 AC-3, ISO/CEI 27001 A.9.1.1 | **Administrateurs système** : Mettre en œuvre les politiques RBAC.
Département RH : Communiquer les changements de rôle des employés.
Équipe de sécurité: Auditez régulièrement les journaux d'accès pour détecter les accès non autorisés. | Phase 1 : Élaboration de politiques (1 mois)
Phase 2 : Déploiement (2 mois)

Phase 3 : Examens d'accès périodiques (trimestriels) | | **Sauvegarde et récupération après sinistre (DR)** | Perte de données, temps d'arrêt du système et temps de récupération prolongés en raison d'incidents tels que des cyberattaques, des catastrophes naturelles ou des pannes matérielles. | - Mettre en œuvre des sauvegardes quotidiennes automatisées pour le stockage de données sur site et hors site.
- Concevoir et tester un plan de reprise après sinistre (DRP) complet, garantissant que les données et les systèmes critiques peuvent être restaurés en 4 heures (RTO).
- Les tests de sauvegarde seront effectués tous les trimestres. | ISO/CEI 27001 A.17.1.2, NIST 800-53 CP-9 | **Opérations informatiques**: Gérer les systèmes de sauvegarde et assurer la disponibilité.
Gestion des risques : Superviser les tests DRP.
Équipes de continuité des activités: S'assurer que le DRP s'aligne sur les priorités organisationnelles. |
Phase 1 : Évaluation de la solution de sauvegarde (1 mois)
Phase 2 : Implémentation (2 mois)
Phase 3 : Tests et mises à jour DRP (3 mois) | | **Protection des points finaux (antivirus et anti-malware)** | Menaces provenant de logiciels malveillants, virus, ransomwares et autres logiciels malveillants ciblant les points finaux. | - Déployer des solutions antivirus et anti-malware sur tous les appareils de point de terminaison (postes de travail, ordinateurs portables, appareils mobiles).
- Mettre à jour et surveiller régulièrement les points de terminaison pour détecter toute activité malveillante.
- Mettre en œuvre des systèmes de détection et de réponse aux points de terminaison (EDR) pour les menaces continues. surveillance. | ISO/CEI 27001 A.12.2.1, NIST 800-53 SI-3 | **Équipe de sécurité des points finaux** : Gérer le déploiement et la configuration.
SOC : Analysez les alertes des points de terminaison et enquêtez sur les activités suspectes.
Administrateurs système : Assurez-vous que le logiciel du point de terminaison est à jour. | Phase 1 : Sélection de la solution (1 mois)
Phase 2 : Déploiement du point de terminaison (3 mois)
Phase 3 : Configuration et surveillance EDR (1 mois) | | **Gestion des informations et des événements de sécurité (SIEM)** | Détection et réponse inadéquates aux événements de sécurité. | - Mettre en œuvre une solution SIEM pour regrouper, corréler et analyser les journaux de tous les périphériques réseau, pare-feu, serveurs et systèmes de protection des points finaux.
- Le SIEM permettra une détection proactive des menaces et permettra des enquêtes médico-légales après l'incident. | NIST 800-53 AU-6, ISO/CEI 27001 A.16.1.1 | **SOC**: Surveiller et gérer SIEM.
Équipe de sécurité informatique : Affinez les règles SIEM.
Administrateurs système: Assurer l'intégration de tous les systèmes avec SIEM. | Phase 1 : Déploiement SIEM (2 mois)
Phase 2 : Intégration aux systèmes (3 mois)
Phase 3 : Suivi et ajustements (En cours) |

---

3. Surveillance continue et amélioration continue

| **Contrôle** | **Activités de surveillance** | **Fréquence** | |---|-- -- --- ---------------------|----------------------| | **Authentification multifacteur (MFA)** | Examinez les tentatives de connexion échouées et surveillez les modèles d’accès suspects. | **Tous les jours** | | **Cryptage des données** | Effectuez des audits sur les clés de chiffrement et surveillez les journaux pour détecter les accès non autorisés ou les tentatives de décryptage. | **Trimestriel** | | **Pare-feu et IDS/IPS** | Examinez et analysez les journaux des tentatives d’intrusion et des événements de sécurité. | **En temps réel** (24h/24 et 7j/7) | | **Contrôle d'accès basé sur les rôles (RBAC)** | Examinez régulièrement les autorisations d’accès des utilisateurs et effectuez un audit pour détecter tout

accès non autorisé ou mauvaise affectation. | **Mensuel** | | **Sauvegarde et récupération après sinistre (DR)** | Vérifiez le succès des sauvegardes, effectuez des tests de restauration et simulez des exercices de reprise après sinistre pour garantir la préparation. | **Hebdomadaire** | | **Protection des points de terminaison** | Surveillez les alertes des points de terminaison, analysez les modèles d'activités malveillantes et assurez-vous que les mises à jour de sécurité des points de terminaison sont appliquées rapidement. | **Tous les jours** | | **Surveillance SIEM** | Examinez les journaux agrégés pour détecter les anomalies, enquêtez sur les incidents et corrélez les données sur plusieurs systèmes pour une analyse précise. | **24h/24 et 7j/7** |

---

4. Amélioration continue

| **Activité** | **

Descriptif** | **Fréquence** | |----------|- ---------- ---------- ---------- ---------- ----------|----------| | **Audits de sécurité** | Réaliser des audits de sécurité et des évaluations de vulnérabilité trimestriels pour vérifier l'efficacité des mesures de sécurité. | **Trimestriel** | | **Formation sur la sécurité des employés** | Formation semestrielle sur la sensibilisation à la cybersécurité, la prévention du phishing, la gestion des mots de passe et la conformité au RGPD. | **Semestriellement** | | **Exercices de réponse aux incidents** | Simulez des scénarios de cyberattaques réels pour évaluer la capacité de l'UNICEF à réagir, à se rétablir et à prévenir les menaces futures. | **Annuellement** | | **Gestion des risques liés aux tiers** | Évaluez et auditez régulièrement les fournisseurs et sous-traitants tiers pour vérifier la conformité en matière de cybersécurité et les mesures de protection des données. | **Annuellement** | | **Flux de renseignements sur les menaces** | Intégrez des informations sur les menaces mondiales dans le SIEM et d'autres systèmes pour garder une longueur d'avance sur les cybermenaces émergentes. | **En cours** |