Portée du système de gestion de la sécurité de l'information (ISMS) de l'UNICEF

---

1. Identifier les actifs informationnels (portée mondiale)

1.1 Inventaire des actifs informationnels

Ordinateurs et appareils

- **Ordinateurs portables et ordinateurs de bureau**:
- **Série Dell Latitude**, **Série HP EliteBook**, **Apple MacBook Pro/iMac** (utilisé par les cadres supérieurs).
- **Systèmes d'exploitation**:
  - **Windows 10/11**: Système d’exploitation principal à l’échelle mondiale.
  - **macOS**: Pour les cadres supérieurs et le personnel spécialisé (ex. : directeurs de programmes).
  - **Linux (Ubuntu)**: Utilisé par certaines équipes techniques dans les régions ayant des besoins en traitement de données à grande échelle.
- **Outil de gestion** : Les appareils sont gérés et suivis à l'aide **Microsoft Intune** pour la sécurité, l’inventaire et la conformité des appareils.

Appareils mobiles

- **Téléphones intelligents**:
- **Modèles Apple iPhone 12/13/14** pour le personnel du programme dans des pays clés comme **Inde**, **Nigeria**, **Syrie**, et **Soudan du Sud**.
- **Appareils Samsung Galaxy** pour les régions d’Amérique latine et les pays dotés d’une infrastructure mobile orientée Android.
- **Gestion mobile** : Appareils inscrits et sécurisés via **VMware AirWatch** pour le cryptage, l’effacement à distance et l’accès sécurisé aux systèmes de l’UNICEF.

Serveurs et bases de données

- **Centres de données mondiaux**:
- **New York (siège)**: Centre de données principal pour les opérations internes mondiales.
- **Genève (Europe)**: Gère les opérations et le stockage des données pour les opérations en Europe, dans la région MENA et dans certaines opérations en Asie-Pacifique.
- **Bureaux régionaux** (par exemple, **Bangkok**, **Nairobi**, **Saint Joseph**) : Pour les besoins locaux de gestion des données et de reprise après sinistre.
- **Infrastructure cloud**:
- **AWS (Amazon Web Services)**:
  - **Instances EC2** (Machines virtuelles) : héberge les opérations mondiales et les systèmes d’intervention d’urgence.

    - **S3** (Simple Storage Service) : stocke de grands ensembles de données pour les programmes de secours d'urgence, de santé infantile et d'éducation à l'échelle mondiale.
    - **RDS** (Service de base de données relationnelle) : héberge des bases de données critiques telles que **Bases de données de l'UNICEF sur la santé, l'éducation et les donateurs**.

- **Microsoft Azure**:
- **Stockage Blob Azure**: Utilisé pour stocker des données financières et des donateurs sensibles.
- **Azure AD** (Active Directory) : gestion centralisée des identités et des accès pour tous les utilisateurs du monde entier.

Applications et logiciels

- **U-Rapport**: Un outil de messagerie sociale pour l'engagement des jeunes dans plus de 50 pays (y compris **Kenya**, **Nigeria**, **Indonésie**).
- **CommCare**: Une application mobile pour la collecte de données sur le terrain, utilisée en cas d'urgence (par ex. **Yémen**, **Soudan du Sud**).
- **SalesforceCRM**: Pour la gestion des dons mondiaux et des relations avec les donateurs.
- **Sauge intacte**: Système financier de suivi des budgets et des dons dans le monde entier.

---

2. Définir les limites physiques

2.1 Emplacements physiques inclus dans le SMSI

- **Siège de l'UNICEF**:
- **New York, États-Unis**: Le bureau principal où sont prises les décisions stratégiques, financières et opérationnelles mondiales.
- **Bureaux régionaux**:
- **Genève, Suisse**: Le hub des opérations européennes, couvrant l'Europe, le Moyen-Orient et l'Asie centrale.
- **Bangkok, Thaïlande**: Gère les opérations pour la région Asie-Pacifique.
- **Nairobi, Kenya**: Gère les opérations pour l’Afrique de l’Est.
- **San José, Costa Rica**: Responsable des programmes Amérique Latine et Caraïbes.
- **Bureaux nationaux**:
- **Inde**: Stockage sécurisé des données et opérations pour l'Asie du Sud (santé, éducation, programmes WASH).
- **Nigeria**: Centres de données en **Abuja**, gérant les données pour l’Afrique de l’Ouest.
- **Syrie**: Données critiques stockées localement sous des protocoles de haute sécurité en raison d'un conflit en cours.

2.2 Zones réglementées

- **Salle de serveurs**: Situé dans les bureaux régionaux et les centres de données nationaux (par ex. **Bangkok**, **Genève**, **Nairobi**) avec accès et surveillance restreints. L'entrée est autorisée uniquement pour les administrateurs système.

---

3. Définir des limites virtuelles

3.1 Sécurité du réseau

- **Le WAN mondial de l'UNICEF**: Réseau étendu sécurisé reliant les bureaux régionaux, les services cloud et les centres de données du monde entier.
- **Réseaux locaux (LAN)**: Dans les bureaux régionaux comme **Bangkok** et **Nairobi** pour assurer la protection locale des données sensibles.

3.2 Environnements cloud

- **Amazon Web Services (AWS)**:
- **Région**: Virginie du Nord (Etats-Unis), Irlande (Europe), Singapour (Asie), Sydney (Australie).
- **Services utilisés**: EC2, S3, Lambda, CloudFront pour des applications cloud évolutives.
- **Microsoft Azure**:
- **Région**: Pays-Bas, Irlande et Amérique du Nord.
- **Services**: Azure Blob Storage pour les données financières et sensibles, Microsoft Teams et Office 365 pour la collaboration et la gestion documentaire.

3.3 Systèmes de sécurité

- **Pare-feu**: Pare-feu de niveau entreprise de **Fortinet** et **Cisco** pour sécuriser le trafic réseau interne et externe.
- **VPN**: **Cisco AnyConnect** Service VPN pour un accès à distance sécurisé aux systèmes de l'UNICEF dans le monde entier.

---

4. Identification des parties prenantes

4.1 Principales parties prenantes

- **Direction exécutive**:

- **Siège de l'UNICEF à New York**: Assure l'alignement avec les objectifs de l'organisation et donne la priorité à la sécurité des informations dans toutes les régions.

- **Équipe informatique mondiale**:

- Basé à **New York**, responsable de la supervision de toutes les politiques de cybersécurité, des évaluations des risques et du contrôle du respect des normes mondiales telles que **ISO 27001**.

- **Équipes informatiques régionales**:

- **Genève**, **Bangkok**, **Nairobi**, **Amman**, et **Saint Joseph**: Des équipes spécifiques à la région gèrent les mises en œuvre locales, la formation du personnel et le reporting.
- **Vendeurs externes**:
- **AWS**, **Microsoft Azure**, **Google Cloud**: Gérer l'infrastructure cloud.
- **Consultants en sécurité**: Travailler avec **KPMG**, **Deloitte** pour les tests d'intrusion et les audits.

---

5. Calendrier de mise en œuvre du SMSI

5.1 Phase 1 : Planification et évaluation des risques (1 à 3 mois)

- **Tâches**:
- Réalisez une évaluation complète des risques des systèmes, infrastructures et données existants.
- Identifier les actifs informationnels clés, en les classant en fonction de **confidentialité**, **intégrité**, et **disponibilité**.
- Concevoir l'architecture du SMSI en accord avec **ISO 27001** normes.
- **Clients livrables**:
- Rapport initial d’évaluation des risques.
- Portée documentée du SMSI.
- Rôles et responsabilités attribués pour l'exécution du SMSI.

5.2 Phase 2 : Élaboration de politiques et mise en œuvre du contrôle (3 à 6 mois)

- **Tâches**:
- Élaborer et mettre en œuvre des politiques de sécurité de l'information couvrant le contrôle d'accès, la protection des données, la réponse aux incidents et la reprise après sinistre.
- Configurez des solutions de sécurité comme **Protection des points de terminaison (CrowdStrike)**, **pare-feu (Fortinet)**, et **authentification multifacteur**.
- Créer des lignes directrices pour l'accès au travail à distance et les opérations sur le terrain (par exemple, en utilisant **AirWatch** pour la gestion des appareils).
- **Clients livrables**:
- Politiques de sécurité publiées.
- Systèmes de sécurité configurés.
- Programmes de sensibilisation du personnel aux procédures de sécurité.

5.3 Phase 3 : Formation et sensibilisation (6 à 9 mois)

- **Tâches**:
- Organiser des séances de formation obligatoires en matière de sécurité pour tout le personnel **hameçonnage**, **gestion des mots de passe**, et **rapport d'incident**.
- Mettre régulièrement à jour la formation en fonction des menaces émergentes (par exemple, webinaires trimestriels sur la sécurité).
- Testez la sensibilisation du personnel avec des campagnes de phishing simulées.
- **Clients livrables**:
- Modules de formation terminés pour tout le personnel.
- Rapports de simulation et résultats d’évaluation.

5.4 Phase 4 : Audits de sécurité et réponse aux incidents (9 à 12 mois)

- **Tâches**:
- Effectuez régulièrement des évaluations de vulnérabilité et des tests d'intrusion avec des fournisseurs de sécurité tiers.
- Mettre en place un système centralisé **Gestion des informations et des événements de sécurité (SIEM)** système comme **Splunk** pour surveiller les journaux et détecter les menaces de sécurité en temps réel.
- Testez les plans de réponse aux incidents en simulant des cyberattaques ou des violations de données.
- **Clients livrables**:
- Rapports d'audit finalisés.
- Procédures de réponse aux incidents.
- Système SIEM configuré et actif.

5.5 Phase 5 : Amélioration continue et surveillance (en cours)

- **Tâches**:
- Mettez régulièrement à jour les politiques ISMS et les mesures de sécurité pour refléter les nouvelles menaces.
- Un suivi permanent avec **Splunk**, **CrowdStrike**et des évaluations périodiques de la vulnérabilité.
- Révision et ajustements annuels du SMSI.
- **Clients livrables**:
- Documentation SMSI mise à jour.
- Rapports d'audit annuels et mises à jour sur la conformité.
- Programmes continus de formation et de sensibilisation du personnel.

---

6. Considérations de conformité et juridiques

- **ISO 27001**: Le SMSI respectera **ISO 27001** normes pour l'établissement, la maintenance et l'amélioration du système de gestion de la sécurité de l'information.
- **RGPD**: Respect des **Règlement général sur la protection des données (RGPD)** pour toute opération impliquant les données des citoyens de l'UE.
- **Autres réglementations locales**: Conformité aux lois locales sur la protection des données dans des régions comme **Afrique (NDPR nigérian)**, **Amérique latine (LGPD du Brésil)**, et **Asie (PDPB indien)**.