UNICEF Information Security Management System (ISMS) - Scope

Purpose: The purpose of this Information Security Management System (ISMS) is to protect the sensitive information and critical assets of UNICEF, ensuring that all operations align with the organization's mission to safeguard children’s rights globally. This system focuses on maintaining confidentiality, data integrity, and availability, alongside mitigating risks to UNICEF's data and systems. Key priorities include:

- Safeguarding personal data of children, staff, and beneficiaries.
- Protecting against unauthorized access to sensitive humanitarian and program data.
- Ensuring the integrity of UNICEF's operations and services to vulnerable populations.
- Supporting compliance with global and regional data privacy laws, including GDPR, and maintaining operational continuity through robust risk management practices.

Scope: This ISMS applies to all UNICEF offices worldwide and encompasses the entire UNICEF ecosystem, including:

- **Headquarters in New York**: The central hub for global policy, strategic decision-making, and high-level data storage.
- **Regional and Country Offices**: Offices in over 190 countries and territories, managing field-based programs and operations, which often involve local-sensitive data.
- **Partnerships**: Collaborations with governments, NGOs, UN agencies, and private sector partners that require secure data sharing and project coordination.

The scope covers the protection of digital and physical assets, from field-based data collection to strategic decision-making systems.

Assets within Scope: The following assets are included within the scope of this ISMS:

1. **Hardware**:
    - UNICEF-managed servers, workstations, mobile devices (smartphones, tablets), printers, routers, firewalls, and switches.
    - Data centers used for storage and processing of UNICEF’s operational data (physical and cloud-based).
2. **Software**:
    - Operating systems (e.g., Windows, Linux, macOS), specialized software for monitoring, reporting, and humanitarian aid tracking.
    - Applications including internal UNICEF systems (e.g., SAP for financial management) and external collaborative platforms such as Microsoft Office 365, Google Workspace, and cloud solutions like Amazon Web Services (AWS).
3. **Data**:
    - Financial records, donor information, human resources data, research data, field-level data, and beneficiary details.

    - Sensitive child protection data and health records collected in partnership with governments and agencies.
    - Reports from UNICEF's diverse programs, including emergency response data during crises (natural disasters, conflict areas, etc.).

4. **Physical Locations**:

    - UNICEF headquarters in New York, regional offices in Geneva, Dakar, and other locations worldwide, and local offices in partner countries.
    - Field offices and mobile units operating in remote and high-risk locations where humanitarian services are provided.

Compliance Requirements

This ISMS is designed to ensure compliance with various global and regional standards, including:

- **General Data Protection Regulation (GDPR)** (Reglamento General de Protección de Datos): The ISMS will ensure compliance with GDPR for handling data related to EU citizens, which is critical for UNICEF's operations in Europe and with EU-based partners.
- **UNICEF's Data Protection and Privacy Policy** (Política de Protección de Datos y Privacidad de UNICEF): This internal policy governs the processing of personal data, ensuring it is handled with due diligence in line with both local and international data protection laws.
- **ISO/IEC 27001**: UNICEF will adhere to ISO/IEC 27001 standards to implement and maintain an effective information security management framework.
- **UN Security Council Resolutions** (Resoluciones del Consejo de Seguridad de la ONU): Compliance with UN resolutions related to information security, especially in conflict zones where security risks may be heightened.
- **Esquema Nacional de Seguridad (ENS)**: Compliance with Spain's **National Security Framework** (ENS) to ensure proper protection of information systems used by public sector organizations in Spain, which applies to UNICEF's operations in the region.

Other regional regulations such as the **Health Insurance Portability and Accountability Act (HIPAA)** (Ley de Portabilidad y Responsabilidad de Seguro de Salud) for healthcare-related data and **National Data Privacy Laws** (Leyes Nacionales de Protección de Datos Personales) in various countries will also be strictly followed.

Exclusions: Certain areas are excluded from the ISMS scope:

- **Third-party vendor data**: Vendors or partners whose services do not involve direct access to UNICEF's critical information systems or data. However, vendors that have direct interactions with sensitive data (e.g., data storage or processing services) must comply with UNICEF's security and privacy standards.
- **Financial transactions**: Transactions handled through external financial institutions, though UNICEF will monitor for fraud and ensure secure systems for financial management.

Responsibilities: Key stakeholders responsible for the implementation and maintenance of the ISMS include:

- **UNICEF Headquarters (New York)**: Overall governance and oversight, ensuring global adherence to security protocols and managing major incident responses.
- **Regional Directors**: Responsible for ensuring that all regional offices comply with the ISMS requirements, conducting regular security audits, and adapting policies to regional threats.
- **Country Office Managers**: Implement ISMS policies at the country level, ensuring that field offices adhere to security measures tailored to local threats.
- **Information Security Officer (ISO)**: Responsible for the ISMS's design, management, and execution, reporting directly to the Chief Information Officer (CIO).

Additional Elements:

1. **Risk Management**: The ISMS includes a robust approach to identifying, assessing, and mitigating risks related to information security. UNICEF will conduct regular risk assessments and audits across its global network, identifying potential vulnerabilities in systems and ensuring timely remediation.

2. **Incident Response**: A defined protocol for responding to security incidents, including data breaches or cyberattacks, ensuring that stakeholders are notified immediately and effective recovery actions are taken. This includes both the internal communication flow and external notification to regulatory bodies when required.

3. **Business Continuity and Disaster Recovery**: The ISMS will ensure business continuity during disruptions. It includes plans for disaster recovery and backups to prevent loss of critical data, particularly in field operations where remote locations and unstable conditions can present unique challenges.