UNICEF Information Security Management System (ISMS) Scope

---

1. Identify Information Assets (Global Scope)

1.1 Inventory of Information Assets

Computers and Devices

- **Laptops and Desktops**:
  - **Dell Latitude Series**, **HP EliteBook Series**, **Apple MacBook Pro/iMac** (used by senior staff).
  - **Operating Systems**:
    - **Windows 10/11**: Primary operating system globally.
    - **macOS**: For senior managers and specialized staff (e.g., program directors).
    - **Linux (Ubuntu)**: Used by some technical teams in regions with large-scale data processing needs.
  - **Management Tool**: Devices are managed and tracked using **Microsoft Intune** for device security, inventory, and compliance.

Mobile Devices

- **Smartphones**:
  - **Apple iPhone 12/13/14 models** for program staff in key countries like **India**, **Nigeria**, **Syria**, and **South Sudan**.
  - **Samsung Galaxy devices** for regions in Latin America and countries with Android-oriented mobile infrastructure.
- **Mobile Management**: Devices enrolled and secured via **VMware AirWatch** for encryption, remote wipe, and secure access to UNICEF systems.

Servers and Databases

- **Global Data Centers**:
  - **New York (HQ)**: Primary data center for internal global operations.
  - **Geneva (Europe)**: Manages operations and data storage for European, MENA, and some Asia-Pacific operations.
  - **Regional Offices** (e.g., **Bangkok**, **Nairobi**, **San José**): For local data management and disaster recovery needs.
- **Cloud Infrastructure**:
  - **AWS (Amazon Web Services)**:
    - **EC2 instances** (Virtual machines): Hosts global operations and emergency response systems.
    - **S3** (Simple Storage Service): Stores large datasets for emergency relief, child health, and education programs globally.

        - **RDS** (Relational Database Service): Hosts mission-critical databases like **UNICEF's health, education, and donor databases**.

    - **Microsoft Azure**:

        - **Azure Blob Storage**: Used for storing sensitive financial and donor data.
        - **Azure AD** (Active Directory): Centralized identity and access management for all users globally.

Applications and Software

- **U-Report**: A social messaging tool for youth engagement in over 50 countries (including **Kenya**, **Nigeria**, **Indonesia**).
- **CommCare**: A mobile app for field data collection, used in emergencies (e.g., **Yemen**, **South Sudan**).
- **Salesforce CRM**: For managing global donations and donor relations.
- **Sage Intacct**: Financial system for tracking budgets and donations worldwide.

---

2. Define Physical Boundaries

2.1 Physical Locations Included in the ISMS

- **UNICEF Headquarters**:

    - **New York, USA**: The primary office where global strategic, financial, and operational decisions are made.

- **Regional Offices**:

    - **Geneva, Switzerland**: The European operations hub, covering Europe, the Middle East, and Central Asia.
    - **Bangkok, Thailand**: Manages operations for the Asia Pacific region.
    - **Nairobi, Kenya**: Handles operations for East Africa.
    - **San José, Costa Rica**: Responsible for Latin American and Caribbean programs.

- **Country Offices**:

    - **India**: Secure data storage and operations for South Asia (health, education, WASH programs).
    - **Nigeria**: Data centers in **Abuja**, managing data for West Africa.
    - **Syria**: Critical data stored locally under high-security protocols due to ongoing conflict.

2.2 Restricted Areas

- **Server Rooms**: Located in regional offices and country data centers (e.g., **Bangkok**, **Geneva**, **Nairobi**) with restricted access and surveillance. Entry is authorized only for system administrators.

---

3. Define Virtual Boundaries

3.1 Network Security

- **UNICEF's Global WAN**: Secure Wide Area Network connecting regional offices, cloud services, and data centers worldwide.
- **Local Area Networks (LANs)**: At regional offices like **Bangkok** and **Nairobi** to ensure local protection of sensitive data.

3.2 Cloud Environments

- **Amazon Web Services (AWS)**:
  - **Region**: North Virginia (US), Ireland (Europe), Singapore (Asia), Sydney (Australia).
  - **Services Used**: EC2, S3, Lambda, CloudFront for scalable cloud applications.
- **Microsoft Azure**:
  - **Region**: Netherlands, Ireland, and North America.
  - **Services**: Azure Blob Storage for financial and sensitive data, Microsoft Teams and Office 365 for collaboration and document management.

3.3 Security Systems

- **Firewalls**: Enterprise-grade firewalls from **Fortinet** and **Cisco** to secure internal and external network traffic.
- **VPN**: **Cisco AnyConnect** VPN service for secure remote access to UNICEF's systems globally.

---

4. Stakeholder Identification

4.1 Key Stakeholders

- **Executive Management**:
  - **UNICEF HQ in New York**: Ensures alignment with organizational goals and prioritizes information security across regions.
- **Global IT Team**:
  - Based in **New York**, responsible for overseeing all cybersecurity policies, risk assessments, and monitoring for compliance with global standards like **ISO 27001**.
- **Regional IT Teams**:
  - **Geneva**, **Bangkok**, **Nairobi**, **Amman**, and **San José**: Region-specific teams manage local implementations, staff training, and reporting.
- **External Vendors**:
  - **AWS**, **Microsoft Azure**, **Google Cloud**: Manage cloud infrastructure.
  - **Security Consultants**: Work with **KPMG**, **Deloitte** for penetration testing and audits.

---

5. ISMS Implementation Timeline

5.1 Phase 1: Planning and Risk Assessment (1–3 Months)

- **Tasks**:
  - Complete a comprehensive risk assessment of existing systems, infrastructure, and data.
  - Identify key information assets, classifying them based on **confidentiality**, **integrity**, and **availability**.
  - Design the ISMS architecture in alignment with **ISO 27001** standards.
- **Key Deliverables**:
  - Initial risk assessment report.
  - Documented scope of ISMS.
  - Assigned roles and responsibilities for ISMS execution.

5.2 Phase 2: Policy Development and Control Implementation (3–6 Months)

- **Tasks**:
  - Develop and implement information security policies covering access control, data protection, incident response, and disaster recovery.
  - Configure security solutions like **endpoint protection (CrowdStrike)**, **firewalls (Fortinet)**, and **multi-factor authentication**.
  - Create guidelines for remote work access and field operations (e.g., using **AirWatch** for device management).
- **Key Deliverables**:
  - Published security policies.
  - Configured security systems.
  - Awareness programs for staff on security procedures.

5.3 Phase 3: Training and Awareness (6–9 Months)

- **Tasks**:
  - Conduct mandatory security training sessions for all staff on **phishing**, **password management**, and **incident reporting**.
  - Regularly update training based on emerging threats (e.g., quarterly security webinars).
  - Test staff awareness with simulated phishing campaigns.
- **Key Deliverables**:
  - Completed training modules for all staff.
  - Simulation reports and assessment outcomes.

5.4 Phase 4: Security Audits and Incident Response (9–12 Months)

- **Tasks**:
  - Conduct regular vulnerability assessments and penetration tests with third-party security providers.
  - Implement a centralized **Security Information and Event Management (SIEM)** system like **Splunk** to monitor logs and detect security threats in real-time.
  - Test incident response plans by simulating cyber-attacks or data breaches.
- **Key Deliverables**:
  - Finalized audit reports.
  - Incident response procedures.

- SIEM system configured and active.

5.5 Phase 5: Continuous Improvement and Monitoring (Ongoing)

- **Tasks**:
  - Regularly update ISMS policies and security measures to reflect new threats.
  - Ongoing monitoring with **Splunk**, **CrowdStrike**, and periodic vulnerability assessments.
  - Annual ISMS review and adjustments.
- **Key Deliverables**:
  - Updated ISMS documentation.
  - Annual audit reports and updates on compliance.
  - Continuous staff training and awareness programs.

---

6. Compliance and Legal Considerations

- **ISO 27001**: The ISMS will adhere to **ISO 27001** standards for establishing, maintaining, and improving the information security management system.
- **GDPR**: Compliance with the **General Data Protection Regulation (GDPR)** for any operations involving EU citizens' data.
- **Other Local Regulations**: Compliance with local data protection laws in regions like **Africa (Nigerian NDPR)**, **Latin America (Brazil’s LGPD)**, and **Asia (India’s PDPB)**.