UNICEF Information Security Management System (ISMS) - Selected Controls

---

1. Access Control

- **Multi-Factor Authentication (MFA)**:
  - **Implementation**: MFA will be required for all access points to UNICEF’s critical systems, applications, and data. This includes both internal and external users, including employees, contractors, and third-party vendors. MFA will combine something the user knows (password), something the user has (smartphone or token), and something the user is (biometric).
  - **Frequency**: MFA will be reviewed monthly to ensure that it is implemented correctly and remains in compliance with UNICEF’s security policies. Any issues identified during reviews will be addressed immediately.
  - **Rationale**: MFA reduces the likelihood of unauthorized access due to stolen or weak credentials by adding multiple layers of verification, significantly enhancing system security.

- **Password Policies**:
  - **Complexity Requirements**: All user passwords must meet the following criteria:
    - A minimum of 12 characters.
    - At least one uppercase letter, one lowercase letter, one number, and one special character.
    - Passwords must not be reused across different systems.
  - **Rotation Frequency**: Passwords must be changed every 90 days, and users are prohibited from using the previous five passwords.
  - **Rationale**: Strong passwords minimize the risk of unauthorized access through brute-force or guessing attacks, while regular password changes mitigate the risks associated with compromised credentials.

- **Role-Based Access Control (RBAC)**:
  - **Implementation**: Access to information and systems will be restricted based on the user's role within the organization. Each employee or contractor will be granted access only to the systems and data necessary for their specific role.
  - **Frequency**: Access permissions will be reviewed quarterly to ensure they align with employees’ current roles and responsibilities. Any discrepancies will be rectified immediately.
  - **Rationale**: RBAC ensures that users can only access data that is relevant to their role, minimizing the risk of unauthorized access and potential data breaches.

---

2. Encryption

- **Data at Rest**:
  - **Implementation**: All sensitive data, including personally identifiable information (PII), financial records, and donor information, will be encrypted using Advanced Encryption Standard (AES) with a key size of 256 bits (AES-256) on local and cloud-based storage.

    - **Retention Period**: Encrypted data will be retained for a minimum of three years. After this period, the data will be reviewed for deletion or further encryption in accordance with data retention policies.
    - **Rationale**: AES-256 provides strong protection for sensitive data, ensuring that even if systems or devices are compromised, unauthorized users cannot access the encrypted data without the proper decryption keys.

- **Data in Transit**:

    - **Implementation**: All communications (email, web traffic, and application data) will be encrypted using Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocols to protect data from eavesdropping and tampering.
    - **Frequency**: A quarterly review of SSL/TLS encryption implementation will be conducted to ensure compliance with the latest security standards. Any outdated protocols (e.g., SSLv3) will be replaced immediately.
    - **Rationale**: Encryption of data in transit ensures that all communications are protected from interception or modification, preserving the integrity and confidentiality of sensitive information while in transit.

---

3. Backup and Recovery

To ensure business continuity, UNICEF will implement a robust backup and recovery strategy, following best practices like the **3-2-1 backup rule**:

Regular Backups

- **Frequency**:

    - **Full Backups**: Weekly
    - **Incremental Backups**: Daily
    - **Critical Data**: Continuous or near-real-time backup for high-priority systems.

- **3-2-1 Rule**:

    - **3 Copies of Data**: 1 primary copy, 2 backup copies.
    - **2 Different Media Types**: On-site (e.g., NAS) and off-site (e.g., cloud).
    - **1 Off-site Copy**: Stored remotely for disaster protection.

- **Retention**: Backups will be stored for **3 years** and securely archived or destroyed when no longer needed.

- **Encryption**: All backup data will be encrypted to ensure confidentiality.

Recovery Testing

- **Frequency**: Conducted **every 6 months**.

- **Recovery Metrics**:

    - **RTO (Recovery Time Objective)**: 4 hours for critical systems.

  - **RPO (Recovery Point Objective)**: 24 hours of potential data loss.
- **Scope**: Simulate real disaster recovery scenarios, test data integrity, and restore systems to ensure full recovery.

Backup Management

- **Monitoring**: Automated tools will ensure backups are completed successfully, with alerts for any failures.
- **Security**: Backup systems will be secured with role-based access, encryption, and audit trails.

---

4. Monitoring and Logging

- **Continuous Monitoring**:
  - **Implementation**: Real-time monitoring will be implemented across all critical systems, networks, and endpoints using intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect and respond to suspicious activities immediately.
  - **Frequency**: Monitoring will occur 24/7, with daily reviews of logs for anomalies and weekly in-depth analyses to identify emerging threats.
  - **Rationale**: Continuous monitoring helps detect potential security incidents early, enabling UNICEF to respond proactively to cyber threats, unauthorized access attempts, and other security events before they escalate.
- **Logging and Audit Trails**:
  - **Implementation**: All critical systems, applications, and network devices will generate detailed logs of user access, system events, and security incidents. These logs will be retained for a minimum of one year to support forensic investigations and compliance audits.
  - **Frequency**: Logs will be reviewed weekly to identify any irregularities, and a comprehensive audit will be conducted annually to ensure the completeness and accuracy of logs.
  - **Rationale**: Logging and maintaining audit trails provide transparency, enabling post-incident investigations and audits to identify root causes of security breaches. Retaining logs supports compliance with regulatory requirements and aids in identifying suspicious activities.

---

5. Incident Response

- **Incident Response Plan**:
  - **Implementation**: UNICEF will maintain a comprehensive, up-to-date incident response plan to address cybersecurity incidents, including data breaches, malware infections, and physical security breaches. The plan will include defined roles and responsibilities, escalation procedures, communication protocols, and recovery procedures.
  - **Frequency**: The incident response plan will be reviewed annually to ensure its effectiveness. Tabletop exercises will be conducted every six months to simulate real-world scenarios and ensure readiness.

- **Rationale**: An effective incident response plan ensures that UNICEF can quickly and efficiently respond to security incidents, minimizing damage, downtime, and reputational harm. Tabletop exercises improve the organization's preparedness for real-world incidents.

- **Threat Intelligence**:
    - **Implementation**: UNICEF will subscribe to relevant threat intelligence feeds to stay updated on the latest cyber threats, vulnerabilities, and attack tactics. This information will be integrated into the incident response plan for proactive defense.
    - **Frequency**: Threat intelligence feeds will be reviewed continuously, and monthly updates will be used to refine security controls.
    - **Rationale**: Integrating threat intelligence into the security framework allows UNICEF to stay ahead of emerging threats and respond to them before they impact operations.

---

6. Physical Security

- **Access Control to Facilities**:
    - **Implementation**: Physical access to UNICEF's offices, server rooms, and data centers will be strictly controlled. Access will be granted only to authorized personnel using ID badges, biometric scanning, and CCTV surveillance.
    - **Frequency**: Access control logs will be reviewed monthly to ensure compliance, and security systems will be tested annually to ensure proper functionality.
    - **Rationale**: Restricting physical access to sensitive facilities helps prevent unauthorized tampering, theft, and other physical security incidents. Strong physical security complements digital security measures, ensuring that all critical infrastructure is protected.

- **Environmental Controls**:
    - **Implementation**: Data centers and critical infrastructure will have environmental controls such as temperature regulation, humidity monitoring, and fire suppression systems.
    - **Frequency**: Environmental systems will be monitored continuously, with annual maintenance checks and system updates.
    - **Rationale**: Ensuring the physical integrity of infrastructure protects against environmental damage (e.g., fire, flooding, or overheating), safeguarding both data and hardware from potential loss.

Conclusion

The selected controls outlined above form a comprehensive framework for ensuring the security, confidentiality, integrity, and availability of information systems and data across UNICEF's global operations. These controls address a wide range of security threats—from cyberattacks to physical security breaches—while emphasizing continuous monitoring, regular testing, and adherence to international standards. By implementing these controls, UNICEF aims to safeguard critical information assets, ensure business continuity, and maintain trust with its stakeholders. Regular reviews, testing, and training will be vital in keeping the ISMS responsive to evolving risks and security challenges.