Security Controls Implementation Plan for UNICEF

1. Review of Relevant Standards and Frameworks

Standard/Framework	Overview	Application	Key Benefits
ISO/IEC 27001: Information Security Management System (ISMS)	An international standard for implementing, operating, and maintaining an ISMS to protect sensitive information.	UNICEF will adopt the ISO/IEC 27001 framework to build a comprehensive ISMS that meets the needs of its operations globally, covering sensitive health records, donor information, and child protection data.	Creates a unified, organization-wide culture of information security; reduces the risk of data breaches and non-compliance; enhances stakeholder trust and global data protection assurance.
NIST SP 800-53: Security and Privacy Controls for Information Systems	A set of federal security and privacy controls designed to protect organizational data and systems across their lifecycle.	UNICEF will integrate NIST SP 800-53 controls to secure systems managing sensitive data and ensure the adoption of best practices across all technology platforms, from network security to data privacy.	Aligns with U.S. government-level standards, provides clear cybersecurity guidelines, and integrates privacy protection with operational security measures.
CIS Controls (Center for Internet Security)	A prioritized set of cybersecurity best practices focused on reducing risks from prevalent cyberattacks.	UNICEF will implement CIS Controls 1-20, ranging from inventory and control of hardware and software to incident response and recovery, to mitigate widespread cyber threats.	Provides an actionable, easy-to-implement set of controls; highly scalable for different parts of the organization; promotes resilience against the most common and dangerous cyber threats.
GDPR (General Data Protection Regulation)	EU regulation that mandates stringent controls over personal data collection, processing, and storage.	UNICEF will comply with GDPR regulations in regions where applicable, particularly concerning EU residents' data, ensuring transparency, security, and accountability in data handling.	Ensures legal compliance in the EU, builds trust with donors and stakeholders, and avoids hefty fines through strict data protection practices.

2. Detailed Security Controls

Control	Risk Addressed	Control Details	Relevant Standards	Roles and Responsibilities	Timeline

Control	Risk Addressed	Control Details	Relevant Standards	Roles and Responsibilities	Timeline
Multi-Factor Authentication (MFA)	Unauthorized access due to compromised credentials.	- Enforce MFA across all critical systems (e.g., UNICEF's global finance system, HR management portals, child protection records). - Required factors: password + OTP (via smartphone or hardware token). - Backup methods like email verification or security questions will be integrated for recovery.	ISO/IEC 27001 A.9.4.2, NIST 800-53 AC-2, CIS Control 16	**IT Security Team**: Deploy and monitor MFA. **HR Department**: Ensure employee compliance. **Security Operations**: Audit MFA effectiveness and respond to issues.	Phase 1: Solution configuration (1 month) Phase 2: Organization-wide MFA deployment (2 months) Phase 3: Testing and adjustments (1 month)

Control	Risk Addressed	Control Details	Relevant Standards	Roles and Responsibilities	Timeline
Data Encryption (At Rest and In Transit)	Data breaches through unauthorized access or interception during transmission/storage.	- All sensitive data (health records, donor data, employee personal details) will be encrypted using AES-256 encryption (at rest) and TLS 1.2/1.3 encryption (in transit). - Key Management System (KMS) will securely handle encryption keys throughout their lifecycle.	ISO/IEC 27001 A.10.1.1, NIST 800-53 SC-12, GDPR Article 32	**IT Security Team**: Implement encryption. **Compliance and Legal Teams**: Ensure encryption methods align with GDPR. **Operations Team**: Regularly audit encryption status and key management.	Phase 1: Tool selection (1 month) Phase 2: Deployment (3 months) Phase 3: Key management implementation (1 month)
Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)	Network-based threats, including unauthorized access, malware, and DoS/DDoS attacks.	- Deploy next-generation firewalls (NGFW) at network entry points. - Implement IDS/IPS to detect and prevent intrusions in real-time. - Integrate threat intelligence feeds for proactive attack detection.	NIST 800-53 AC-4, CIS Control 9, ISO/IEC 27001 A.13.1.1	**Network Security Team**: Configure firewalls and IDS/IPS. **SOC**: Monitor network traffic and identify threats. **System Admins**: Ensure firewalls and IPS are configured and tested properly.	Phase 1: Initial installation (2 months) Phase 2: Regular updates and performance optimization (Ongoing)

Control	Risk Addressed	Control Details	Relevant Standards	Roles and Responsibilities	Timeline
Role-Based Access Control (RBAC)	Unauthorized access due to failure to enforce least-privilege access control.	- Implement RBAC for all systems, ensuring users have access to only the data necessary for their roles. - Leverage Active Directory or LDAP for centralized access control. - Periodic audits to ensure access remains in line with job responsibilities.	NIST 800-53 AC-3, ISO/IEC 27001 A.9.1.1	**System Admins**: Implement RBAC policies. **HR Department**: Communicate employee role changes. **Security Team**: Audit access logs regularly to detect unauthorized access.	Phase 1: Policy development (1 month) Phase 2: Deployment (2 months) Phase 3: Periodic access reviews (Quarterly)
Backup and Disaster Recovery (DR)	Data loss, system downtime, and extended recovery times due to incidents like cyberattacks, natural disasters, or hardware failures.	- Implement automated, daily backups to both on-site and off-site data storage. - Design and test a comprehensive Disaster Recovery Plan (DRP), ensuring that mission-critical data and systems can be restored in 4 hours (RTO). - Backup testing will be performed quarterly.	ISO/IEC 27001 A.17.1.2, NIST 800-53 CP-9	**IT Operations**: Manage backup systems and ensure availability. **Risk Management**: Oversee DRP testing. **Business Continuity Teams**: Ensure DRP aligns with organizational priorities.	Phase 1: Backup solution evaluation (1 month) Phase 2: Implementation (2 months) Phase 3: DRP testing and updates (3 months)

Control	Risk Addressed	Control Details	Relevant Standards	Roles and Responsibilities	Timeline
Endpoint Protection (Antivirus and Anti-Malware)	Threats from malware, viruses, ransomware, and other malicious software targeting endpoints.	- Deploy antivirus and anti-malware solutions on all endpoint devices (workstations, laptops, mobile devices). - Regularly update and monitor endpoints for malicious activity. - Implement endpoint detection and response (EDR) systems for continuous threat monitoring.	ISO/IEC 27001 A.12.2.1, NIST 800-53 SI-3	**Endpoint Security Team**: Manage deployment and configuration. **SOC**: Analyze endpoint alerts and investigate suspicious activities. **System Admins**: Ensure endpoint software is up-to-date.	Phase 1: Solution selection (1 month) Phase 2: Endpoint deployment (3 months) Phase 3: EDR setup and monitoring (1 month)
Security Information and Event Management (SIEM)	Inadequate detection and response to security events.	- Implement a SIEM solution to aggregate, correlate, and analyze logs from all network devices, firewalls, servers, and endpoint protection systems. - The SIEM will enable proactive threat detection and enable forensic investigations post-incident.	NIST 800-53 AU-6, ISO/IEC 27001 A.16.1.1	**SOC**: Monitor and manage SIEM. **IT Security Team**: Fine-tune SIEM rules. **System Admins**: Ensure integration of all systems with SIEM.	Phase 1: SIEM deployment (2 months) Phase 2: Integration with systems (3 months) Phase 3: Monitoring and adjustments (Ongoing)

3. Ongoing Monitoring and Continuous Improvement

Control	Monitoring Activities	Frequency
Multi-Factor Authentication (MFA)	Review failed login attempts and monitor suspicious access patterns.	**Daily**
Data Encryption	Perform audits on encryption keys and monitor logs for unauthorized access or decryption attempts.	**Quarterly**
Firewalls & IDS/IPS	Review and analyze logs for intrusion attempts and security events.	**Real-Time** (24/7)
Role-Based Access Control (RBAC)	Regularly review user access permissions and audit for unauthorized access or misassignments.	**Monthly**
Backup & Disaster Recovery (DR)	Verify success of backups, conduct restoration tests, and simulate disaster recovery exercises to ensure readiness.	**Weekly**
Endpoint Protection	Monitor endpoint alerts, analyze malicious activity patterns, and ensure endpoint security updates are applied promptly.	**Daily**
SIEM Monitoring	Review aggregated logs for anomalies, investigate incidents, and correlate data across multiple systems for accurate analysis.	**24/7**

4. Continuous Improvement

| **Activity** | **

Description**	Frequency
Security Audits	Conduct quarterly security audits and vulnerability assessments to verify the effectiveness of security measures.
Employee Security Training	Bi-annual training on cybersecurity awareness, phishing prevention, password management, and compliance with GDPR.
Incident Response Drills	Simulate real-world cyberattack scenarios to evaluate UNICEF’s ability to respond, recover, and prevent future threats.
Third-Party Risk Management	Regularly assess and audit third-party vendors and contractors for cybersecurity compliance and data protection measures.
Threat Intelligence Feeds	Incorporate global threat intelligence feeds into SIEM and other systems to stay ahead of emerging cyber threats.