UNICEF Security Policies & Procedures

Table of Contents

---

1. **Introduction to UNICEF's Security Framework**

The **UNICEF Information Security Practices Framework** is designed to ensure that UNICEF's digital infrastructure, sensitive data, and resources are effectively protected from threats and risks, including cyberattacks, data breaches, natural disasters, and human error. Given its global presence in child protection, health, education, and humanitarian efforts, UNICEF requires robust and comprehensive security measures.

- **Vision**: To protect UNICEF’s sensitive data, support global operations, ensure the safety of children worldwide, and maintain the trust of stakeholders.
- **Core Elements**:
  - **Data Privacy**: Compliance with global data privacy standards (GDPR, HIPAA, etc.).
  - **Incident Response**: Establishing clear, organized processes for detecting, managing, and mitigating incidents.
  - **Business Continuity**: Ensuring minimal disruption to UNICEF’s mission-critical operations during a crisis.
  - **Security Awareness**: Ongoing training to reduce human errors and maintain a vigilant, well-informed workforce.

---

2. **Governance and Compliance**

2.1 Key Regulations and Compliance Frameworks

UNICEF operates in diverse regions and jurisdictions, each with its own data protection laws and cybersecurity regulations. The organization aligns its security practices with the following key standards:

- **ISO/IEC 27001**: This standard outlines best practices for an **Information Security Management System (ISMS)**. UNICEF ensures the framework provides robust security controls, from identifying risks to implementing mitigations.
- **General Data Protection Regulation (GDPR)**: Compliance with GDPR is mandatory for handling personal data of EU citizens. UNICEF's processes are designed to uphold rights such as data minimization, transparency, and accountability.
    - Example: UNICEF provides individuals with clear consent forms and rights to access and delete their data, in line with GDPR requirements.
- **NIST SP 800-53**: A U.S. federal standard that provides a catalog of security controls for federal information systems, ensuring compliance with cybersecurity requirements.
- **CIS Critical Security Controls**: A set of prioritized cybersecurity best practices that UNICEF follows to secure its systems against common vulnerabilities and threats.
- **Health Insurance Portability and Accountability Act (HIPAA)**: Applicable to UNICEF's medical data handling in specific humanitarian contexts (e.g., providing health services to children), requiring stringent protections for health information.

2.2 Security Governance Structure

The **Security Governance Structure** within UNICEF is a multifaceted and comprehensive approach designed to ensure that information security is embedded at every level of the organization. This structure provides leadership, oversight, and accountability for security decisions, and ensures that UNICEF's security efforts align with its organizational objectives and global regulatory requirements. The following components define this governance framework:

CISO (Chief Information Security Officer)

The **Chief Information Security Officer (CISO)** holds the ultimate responsibility for the overall security strategy, leadership, and execution of security initiatives across UNICEF. The CISO is responsible for ensuring that all aspects of information security, from threat management to compliance with international standards, are covered and effectively implemented.

Key Responsibilities:

- **Strategic Oversight**: The CISO ensures that the information security program aligns with UNICEF's mission and operational needs. They develop long-term security strategies, ensuring resources are allocated effectively and risks are managed proactively.
- **Risk Management**: The CISO assesses risks and vulnerabilities related to UNICEF's digital and physical assets, including data, networks, and intellectual property. They create and update risk mitigation strategies and are responsible for making decisions about acceptable levels of risk.
- **Compliance & Regulations**: The CISO ensures UNICEF meets global standards such as **GDPR**, **ISO/IEC 27001**, **NIST SP 800-53**, and **HIPAA** (when applicable), while ensuring compliance with the security and data privacy laws of various countries UNICEF operates in.
- **Reporting to Executive Leadership**: The CISO provides regular security reports to UNICEF's executive leadership and Board of Directors, including updates on security risks, incidents, and strategic initiatives.

Integration into Risk Management Committee:

The CISO is a key member of UNICEF's **Risk Management Committee**. This committee is responsible for strategic decisions on organizational risk, cybersecurity, and data privacy, integrating security into the organization's overall risk management framework. The Risk Management Committee meets regularly to discuss emerging threats, regulatory changes, and the organization's readiness to handle risks.

Security Operations Center (SOC)

The **Security Operations Center (SOC)** is the backbone of UNICEF's security operations, tasked with monitoring and responding to real-time security incidents. The SOC team operates 24/7, employing state-of-the-art tools and technologies to monitor all critical systems and infrastructure.

Key Functions:

- **Real-time Threat Detection**: The SOC uses advanced security tools such as **Splunk** for log aggregation and analysis, **CrowdStrike** for endpoint protection, and **AWS GuardDuty** for cloud threat intelligence. These tools continuously monitor security events, detect abnormal activities, and issue alerts for immediate action.
    - **Splunk**: It helps in **Security Information and Event Management (SIEM)**, aggregating data from multiple sources (servers, endpoints, applications) to identify potential security incidents like data breaches, denial-of-service attacks, or insider threats.
    - **CrowdStrike Falcon**: A key tool for endpoint security that provides real-time monitoring of devices used by staff, such as laptops and mobile phones, to detect and mitigate malware, ransomware, and other endpoint threats.
- **Incident Detection & Response**: The SOC detects suspicious activities, analyzes potential threats, and coordinates with the Incident Response Team (IRT) to contain, mitigate, and resolve incidents promptly.
    - Example: If the SOC detects an unusual data exfiltration attempt through network monitoring, the team instantly alerts the IRT to take action, such as isolating the affected system and blocking further data transfer.
- **Threat Intelligence**: The SOC continuously integrates threat intelligence feeds from global security providers and internal sources to anticipate emerging threats. Tools like **FireEye** and **ThreatConnect** are used to gather and analyze information about new threats targeting organizations like UNICEF.
- **Proactive Monitoring & Hunting**: In addition to reactive monitoring, the SOC proactively searches for potential vulnerabilities and signs of compromise, using techniques like **Threat Hunting** and **Red Teaming** exercises to test and improve security defenses.

SOC Staffing:

The SOC is composed of **Security Analysts**, **Incident Responders**, **Threat Intelligence Specialists**, and **Forensics Experts** who work together to ensure the availability, integrity, and confidentiality of UNICEF's data and systems.

IT Security Committee

The **IT Security Committee** is a cross-functional group consisting of senior IT and security professionals within UNICEF. The committee's primary responsibility is to oversee the formulation, implementation, and review of the organization's security strategy, policies, and operational plans.

Key Responsibilities:

- **Strategic Planning**: The IT Security Committee works with the CISO to define and update the organization's security strategy, identifying key areas for improvement and ensuring alignment with the organization's broader objectives.
- **Security Policy Development**: The committee plays a crucial role in drafting and reviewing security policies, including data protection, encryption standards, user access controls, and security incident management protocols.
- **Security Budget and Resource Allocation**: The committee decides on security-related investments, evaluating funding for necessary tools, training, and security operations. They prioritize budget allocation to ensure resources are directed towards high-priority initiatives such as infrastructure upgrades or new security tools.
- **Risk Assessment & Mitigation**: The committee evaluates the effectiveness of the organization's risk management efforts, considering the evolving landscape of cybersecurity threats, regulatory changes, and UNICEF's operational risk exposure.
- **Security Posture Evaluation**: The IT Security Committee works with external auditors to review the current security posture of the organization, ensuring that critical systems are protected against potential vulnerabilities and threats.

Key Stakeholders in the IT Security Committee:

- **CTO (Chief Technology Officer)**: Works closely with the CISO to align technical infrastructure and innovations with security needs.
- **Legal and Compliance Officers**: Ensure that security initiatives comply with international laws and industry regulations, like GDPR and ISO/IEC standards.
- **Risk Management Team**: Collaborates with the committee to identify and address emerging risks to the organization's information assets.
- **External Experts**: Occasionally, the committee consults with external experts such as **security consultants**, **penetration testers**, or **compliance auditors** to evaluate and improve security practices.

External Auditors

External auditors play an integral role in ensuring that UNICEF's information security practices remain effective and compliant with the highest standards. They bring an independent, unbiased perspective to security governance, and are critical in identifying gaps and vulnerabilities.

Key Roles and Responsibilities:

- **Compliance Audits**: UNICEF engages with third-party auditors like **KPMG**, **PwC**, and **Deloitte** to conduct periodic audits, assessing the organization's compliance with major security regulations and frameworks such as **ISO 27001**, **SOC 2**, **GDPR**, and **NIST SP 800-53**.
    - Example: A **PwC audit** of UNICEF's cloud security posture evaluates whether the organization's cloud configurations adhere to best practices and regulatory standards for data protection.
- **Vulnerability Assessments & Penetration Testing**: External auditors are often tasked with conducting comprehensive security assessments, which include **penetration testing**, **vulnerability scanning**, and **code review**. These assessments help UNICEF identify potential weaknesses in its digital infrastructure.
    - Example: A **penetration test** might uncover security gaps in UNICEF's mobile application or web portals, leading to recommendations for more robust encryption and authentication mechanisms.
- **Gap Analysis**: After completing their assessments, external auditors conduct gap analysis reports, highlighting areas of vulnerability and advising on necessary improvements or corrective actions.

    - Example: The auditors may identify that UNICEF's endpoint protection measures need strengthening to account for the growing use of **mobile devices** for remote operations in the field.
- **Reporting to the Board**: External auditors provide independent reports on the effectiveness of the information security program, offering recommendations for continuous improvement. These reports are often presented directly to UNICEF's senior management and board of directors.

Benefits of External Audits:

- **Independent Verification**: External audits provide a neutral, third-party review of UNICEF's security controls and practices, which helps ensure that the organization's systems are secure and compliant.
- **Regulatory Assurance**: Regular engagement with auditors helps UNICEF prove its commitment to compliance with international data protection laws and industry standards.
- **Ongoing Security Improvements**: Findings from external audits feed directly into UNICEF's continuous improvement cycle, enhancing the security posture over time.

Integration with Other Governance Structures

In addition to these specific roles, UNICEF's security governance framework is integrated with broader organizational structures, ensuring that cybersecurity considerations are incorporated into all decision-making processes. The **Information Technology (IT) Governance** structure works closely with security teams to ensure that new technologies and systems are evaluated for security risks before being implemented.

---

3. Information Security Policy

3.1 Purpose and Scope

The **Information Security Policy** defines UNICEF's comprehensive approach to safeguarding its information and technology assets. This policy ensures the confidentiality, integrity, and availability of the organization's information and systems, while adhering to global compliance and privacy regulations. The policy applies to:

- **Employees**: This includes all full-time employees, contractors, temporary workers, interns, and third-party service providers who have access to UNICEF's information systems. All staff members are required to familiarize themselves with the policy and follow security procedures.

    - **Example**: A contractor working on a project for UNICEF must adhere to the same security protocols as full-time staff, including access control measures and incident reporting requirements.

- **Systems**: All systems operated or owned by UNICEF, including:

    - **IT infrastructure**: Internal servers, network devices, firewalls, and data storage systems.
    - **Cloud systems**: Any services hosted on cloud platforms like **Amazon Web Services (AWS)**, **Microsoft Azure**, and **Google Cloud Platform (GCP)**, where UNICEF's critical applications and data are stored.
    - **Endpoints**: All devices such as laptops, desktops, tablets, smartphones, and other connected equipment that can access UNICEF's internal networks and services.
    - **Networks**: All internal and external communication networks, including virtual private networks (VPNs) used by UNICEF staff for remote work and secure access.

- **Data**: The policy covers all types of data handled by UNICEF, including:

- **Personal Data**: Data subject to privacy regulations such as the **General Data Protection Regulation (GDPR)**, which covers personal data related to UNICEF donors, employees, and beneficiaries.
- **Operational Data**: Includes project data, internal communications, and research information.
- **Sensitive Financial Information**: All financial records, budgets, payroll data, and other sensitive financial details.
- **Intellectual Property**: Documents, designs, software, and other materials developed by UNICEF.

3.2 Security Objectives

The information security policy is designed to achieve the following security objectives:

Confidentiality

Confidentiality ensures that sensitive information is only accessible to those with authorized access, reducing the risk of unauthorized disclosure. UNICEF employs a **multi-layered security approach** to enforce confidentiality at every level of its information ecosystem.

- **Data Encryption**: All sensitive personal data and operational information are encrypted at rest and in transit using strong encryption protocols.
  - **Example**: Personal data such as donor information and beneficiary records are encrypted at rest using **AWS Key Management Service (KMS)** with **AES-256** encryption. Data in transit is encrypted using **Transport Layer Security (TLS)**.
- **Access Control**: Access is granted based on the **least privilege principle**, ensuring employees only have access to the data necessary for their specific roles.
  - **Example**: Employees in the finance department can only access financial records, while HR staff can access employee data but not financial data. Access rights are managed through **Okta** and are reviewed regularly.
- **Data Masking & Redaction**: For certain sensitive operations (e.g., public-facing reports, data shared with partners), sensitive fields are masked or redacted to prevent unauthorized access.
  - **Example**: Donor information in reports shared with external partners is masked to protect personal identities.

Integrity

Integrity ensures that information is accurate, consistent, and trustworthy throughout its lifecycle. To protect data integrity, UNICEF employs several measures:

- **Data Validation and Checksums**: To verify the authenticity of critical data, UNICEF uses cryptographic hashes (e.g., **SHA-256**) and checksums during data transfers or processing.
  - **Example**: When transferring large datasets across platforms or back up data, UNICEF generates cryptographic hashes to verify that the data has not been tampered with during transmission.
- **Version Control**: Changes to critical documents, codebases, and data are tracked using version control systems such as **GitHub** for code and **SharePoint** for documents.
  - **Example**: A change to UNICEF's internal financial forecast is logged, and any discrepancies are flagged for review.

Availability

Availability ensures that information and systems are accessible to authorized users when needed, minimizing downtime and service interruptions.

- **High Availability Systems**: UNICEF implements high availability setups for mission-critical systems, ensuring minimal downtime in case of failure. For example, **SAP** and **Salesforce** are deployed on **AWS** infrastructure using multi-availability zone (AZ) deployments, ensuring redundancy and failover capabilities.
    - **Example**: If an AWS AZ fails, traffic is automatically rerouted to another available zone within the region, ensuring continuous service availability.
- **Disaster Recovery**: A robust disaster recovery plan is in place, with frequent backups of critical data and systems to ensure that recovery objectives are met within acceptable timeframes (Recovery Time Objectives - RTO) and data loss is minimized (Recovery Point Objectives - RPO).
    - **Example**: UNICEF performs daily backups of data and systems using **Veeam Backup** to replicate data across **AWS S3** buckets and **AWS Glacier** for long-term storage. These backups are tested regularly for data integrity and restoration.

Non-repudiation

Non-repudiation ensures that actions performed on systems and data are traceable, providing accountability and preventing users from denying their actions.

- **Audit Trails**: All user interactions with sensitive systems and data are logged. The logs are aggregated and stored securely for forensic analysis if required. Tools like **Splunk** are used to monitor and analyze user activities, generating alerts for any anomalous or suspicious actions.
    - **Example**: If an employee accesses a donor's financial data, an entry is created in the **Splunk** log, capturing the identity of the user, the time, and the type of action taken (e.g., read, write, update).
- **Digital Signatures**: Documents and transactions requiring signatures are digitally signed to ensure authenticity and to prevent tampering. This includes agreements, contracts, and key communications.
    - **Example**: UNICEF uses **DocuSign** for signing official documents, ensuring that each document has an encrypted digital signature that can’t be altered.

3.3 Risk Assessment and Management

- **Continuous Risk Assessment**: UNICEF conducts ongoing risk assessments to identify potential security threats to its systems and data. These assessments are designed to prioritize vulnerabilities based on the potential impact to the organization and the likelihood of occurrence.
    - **Example**: Every year, UNICEF runs a **risk assessment** that includes vulnerability scans using tools such as **Qualys** and **Tenable.io**, followed by an in-depth **penetration testing** engagement with an external security firm like **KPMG**.
- **Security Audits**: Periodic internal and external security audits are conducted to ensure compliance with industry standards and organizational policies.
    - **Example**: **PwC** performs an annual security audit of UNICEF's IT infrastructure to ensure compliance with **ISO 27001** and **SOC 2** standards.
- **Vulnerability Management**: Vulnerabilities identified during scans or audits are prioritized and remediated in a timely manner. Critical vulnerabilities that pose significant risk to systems are addressed within **24 hours**.
    - **Example**: If a critical vulnerability is identified in **SAP** during an audit, the vulnerability management team works to patch it within the defined timeline to mitigate the potential risk.

3.4 Employee and Contractor Compliance

All UNICEF employees, contractors, and third-party vendors are required to comply with the **Information Security Policy**. This includes adherence to:

- **Training Programs**: All employees undergo annual security awareness training via platforms like **KnowBe4**, focusing on identifying phishing, understanding password security, and reporting potential security incidents.
    - **Example**: Every new employee is required to complete a security onboarding course within the first month of employment, which includes modules on acceptable use policies, data protection, and system access control.
- **Third-Party Management**: Contractors and third-party vendors must sign confidentiality agreements, undergo security screenings, and comply with UNICEF's security policies when working with sensitive data.
    - **Example**: Before a third-party vendor is granted access to UNICEF's data, a **third-party risk assessment** is performed to evaluate their security posture and ensure they comply with UNICEF's information security standards.

3.5 Policy Enforcement and Violations

- **Enforcement**: The **CISO** and the **IT Security Committee** are responsible for enforcing the Information Security Policy. Any violations of the policy can result in disciplinary action, including termination, legal action, or financial penalties.
    - **Example**: If an employee is found to have violated data access controls by improperly sharing sensitive data, they may be subject to a formal investigation and potential termination.
- **Monitoring & Reporting**: UNICEF continuously monitors its systems for compliance with the policy using automated tools like **Splunk** and manual audits. Employees are encouraged to report any suspicious activities or breaches through designated reporting channels.
    - **Example**: Employees can report a suspected phishing attempt via the company's security email or an internal ticketing system, which will trigger an investigation.

3.6 Policy Review and Updates

- **Periodic Review**: The Information Security Policy is reviewed annually and updated as necessary to address emerging threats, new compliance requirements, and advancements in technology.
    - **Example**: After a major global cybersecurity event like the **SolarWinds attack**, UNICEF's security policies are reviewed and updated to ensure that the organization is protected against similar types of attacks.
- **Feedback Mechanism**: Employees, contractors, and external auditors are encouraged to provide feedback on the policy and suggest improvements, which are considered during the annual review.
    - **Example**: After a phishing attack campaign, the **CISO** holds a feedback session with key employees to discuss what went wrong and how the policy can be updated to improve security awareness.

---

4. User Access Control & Authentication

4.1 Identity and Access Management (IAM)

UNICEF adopts a robust and centralized **Identity and Access Management (IAM)** framework to manage user identities, authentication, and access controls across all systems and applications. The IAM system ensures that only authorized individuals have access to sensitive information and resources, based on their roles and responsibilities within the organization. It helps mitigate the risk of unauthorized access, data breaches, and insider threats.

Okta - Centralized IAM Platform

UNICEF leverages **Okta** as its primary IAM solution, which integrates with a variety of enterprise systems, ensuring seamless and secure authentication for users across all platforms and services. Okta provides **Single Sign-On (SSO)** and **Multi-Factor Authentication (MFA)**, allowing users to securely access multiple systems without needing separate passwords for each one.

- **Single Sign-On (SSO)**: Okta's SSO functionality enables users to log in once and gain access to a wide array of applications, minimizing the need to remember multiple usernames and passwords.
    - **Example**: A UNICEF employee can log into Okta using their credentials and access a suite of tools like **Workday** for HR tasks, **Salesforce** for donor management, and **Slack** for team communication, without the need to enter separate credentials for each.
    - **Benefit**: This enhances the user experience, reduces login fatigue, and increases security by minimizing password-related vulnerabilities.
- **Multi-Factor Authentication (MFA)**: MFA is enforced for all users accessing sensitive systems. MFA requires users to provide two or more verification factors, adding an additional layer of security. This can include a combination of something the user knows (password), something the user has (mobile device or security token), or something the user is (biometric data like fingerprints or facial recognition).
    - **Example**: When a UNICEF employee accesses their payroll system via **Workday**, they are prompted to enter their password and then authenticate via an MFA method, such as a code sent to their phone via SMS or an app like **Google Authenticator**.
    - **Benefit**: MFA significantly reduces the risk of unauthorized access, even if an attacker acquires a user's password.

Role-Based Access Control (RBAC)

UNICEF employs **Role-Based Access Control (RBAC)** to ensure users have access only to the resources and data necessary for their specific job functions. RBAC minimizes the risk of data leakage or unauthorized access by limiting what users can see and do based on their role within the organization.

- **Granular Role Definitions**: Roles are carefully defined within the IAM system to reflect various job functions, departments, and security requirements. Roles are mapped to specific applications and permissions, ensuring that users can only access the data and functions relevant to their role.
    - **Example**: A **HR Manager** might have access to employee records and payroll data but will not be able to view financial reports, which are restricted to the **Finance Team**.
    - **Example**: An **IT Administrator** has broad access to system settings and configurations but will not have access to HR or payroll systems, which are not part of their job responsibilities.

- **Least Privilege Principle**: Access rights are provided based on the **least privilege** principle, meaning users are granted only the minimal level of access necessary for them to perform their job functions. Access levels are periodically reviewed and adjusted to ensure they remain appropriate.
    - **Example**: A contractor hired for a short-term project will be given limited access to the project files on **SharePoint**, without access to the organization's broader network or sensitive financial systems.

Federated Identity Management

In addition to Okta, UNICEF also utilizes **Federated Identity Management** for secure access to external services, allowing employees to use their corporate credentials to access third-party platforms without creating separate accounts.

- **Example**: UNICEF employees can access cloud-based platforms like **AWS** or **Google Cloud Platform (GCP)** using their Okta credentials, streamlining access while ensuring centralized management of permissions.

4.2 Password Management Policies

Effective password management is critical to safeguarding user accounts and systems from unauthorized access. UNICEF enforces strong password policies to ensure that passwords are complex and secure while providing an efficient process for users to manage their credentials.

Password Complexity Requirements

UNICEF mandates that passwords meet stringent complexity requirements to ensure robustness against common password-guessing attacks (e.g., brute force and dictionary attacks).

- **Password Length & Character Diversity**: All passwords must be at least **12 characters** long and include a combination of:
    - Uppercase and lowercase letters
    - Numbers (at least one)
    - Special characters (e.g., @, #, $, %, &, etc.)
    - **Example**: A password like "UNICEF$2024!Secure" meets these requirements, offering a high level of complexity to resist common attacks.
- **Password Blacklists**: UNICEF employs a password blacklist to prevent users from selecting weak or commonly used passwords that are easily guessable. Common passwords like "password123" or "qwerty" are automatically flagged and rejected by the system.
    - **Example**: If a user attempts to set their password as "12345678," the system will prevent them from doing so and prompt them to select a stronger password.

Password Expiry and Rotation

To further protect accounts from unauthorized access due to password theft or compromise, UNICEF enforces periodic password expiration.

- **Password Expiry Interval**: All user passwords expire every **90 days** to ensure that old passwords are not left vulnerable indefinitely. Users are notified 10 days in advance of password expiration and are

required to update their passwords within this period.

    - **Example**: A user is notified by **Okta** via email and in-app reminders that their password is expiring in 10 days. They are prompted to choose a new password that complies with the complexity requirements.

- **Password History**: Users are prohibited from reusing the same password within a certain number of password changes (e.g., 5 previous passwords) to prevent the recycling of insecure passwords.

    - **Example**: After a user resets their password, they are not allowed to revert to a previously used password, thereby promoting the creation of new, secure passwords.

Password Recovery Process

To ensure that users can securely recover access to their accounts without compromising security, UNICEF employs a robust **password recovery** process that incorporates **Multi-Factor Authentication (MFA)**.

- **Recovery Method**: If a user forgets their password, they can use the **Okta self-service portal** to initiate the password recovery process. The user must authenticate using a second factor, such as a verification code sent to their registered phone number or email.

    - **Example**: A user who forgets their password is prompted to enter their email address. They will receive an authentication code via **SMS** or **email**, which they must enter in order to reset their password securely.

- **Time-Based Recovery Tokens**: The recovery process uses **time-based one-time passwords (TOTP)**, ensuring that any recovery tokens sent to users are valid for only a short window, further enhancing security.

    - **Example**: A user requesting a password reset will receive a 6-digit TOTP that expires within 10 minutes, preventing an attacker from intercepting and reusing the code.

Password Management Tools

UNICEF also encourages the use of **Password Managers** for users to securely store and manage their complex passwords. Tools like **1Password** or **LastPass** can help users maintain strong, unique passwords for each application without the risk of forgetting them.

- **Example**: A user accesses their **Salesforce** account and uses a password manager to generate a unique password, which is securely stored and auto-filled for future logins.

4.3 Access Auditing and Monitoring

Regular monitoring and auditing of user access activities help ensure that users are adhering to security policies and allow for the detection of potential security incidents, such as unauthorized access or suspicious behavior.

- **Audit Logs**: Okta maintains detailed **audit logs** for all user authentication and access activities, which are centrally stored and analyzed for anomalies. These logs include information such as login attempts, failed login attempts, IP addresses, and time stamps.

    - **Example**: If a user accesses a sensitive system like **SAP**, the system logs every action taken by the user. If an unusual number of failed login attempts is detected, a **security alert** is triggered for review.

- **Real-Time Monitoring**: Integration with tools like **Splunk** or **CrowdStrike** allows for real-time monitoring of user access across all systems. Alerts are automatically triggered when suspicious access patterns (e.g., multiple failed logins, access from unusual IPs) are detected.

    - **Example**: If an employee logs in from an unfamiliar location or device, the system flags this activity and requests additional verification via **Okta MFA** before granting access.

- **Periodic Access Reviews**: Regular **access reviews** ensure that users maintain appropriate access rights based on their current roles and responsibilities. Access to critical systems and data is periodically reviewed by the security team and department heads.

    - **Example**: Every quarter, the **HR department** reviews access privileges for all employees, ensuring that users who have changed roles or left the organization have their access promptly revoked.

---

5. Incident Response Plan (IRP)

5.1 Incident Management Lifecycle with Timelines

Incident Type	Detection Tools	Actions	Next Steps	Pre-Incident Planning	Response Timeline
Unauthorized Access (Brute Force, Account Compromise)	- **Okta**: Failed login attempts. - **CrowdStrike**: Unusual activity. - **AWS GuardDuty**: Anomaly detection.	- Lock affected account. - Trigger **forced password reset**. - Isolate compromised systems.	- Forensic analysis of logs to identify lateral movement. - Notify impacted users.	- Enforce **MFA**. - Implement **advanced login detection**.	**Immediate (5-15 mins)** for detection. **30 mins** for containment. **1-2 hours** for eradication. **4-12 hours** for recovery.

Incident Type	Detection Tools	Actions	Next Steps	Pre-Incident Planning	Response Timeline
Malware Infection (Ransomware, Trojans)	- **CrowdStrike Falcon**: Endpoint detection. - **Splunk**: Abnormal traffic. - **AWS GuardDuty**: Suspicious activity.	- Isolate affected device. - Run **full malware scan**. - Analyze system logs for malware behavior.	- **Reimage** affected machines. - Notify internal stakeholders. - Remediate root cause.	- Deploy **ATP**. - Regular **offline backups**. - **Network segmentation**.	**Immediate (5-15 mins)** for detection. **30-60 mins** for containment. **1-4 hours** for eradication. **4-12 hours** for recovery.
Phishing Attack (Credential Harvesting)	- **Mimecast**: Malicious email filter. - **Splunk**: Correlating abnormal network traffic. - **Proofpoint**: Phishing detection.	- Quarantine malicious email. - Trigger password reset for affected users. - Review email source & DNS logs.	- Run security sweep of affected devices. - Notify other users to be cautious. - Analyze and report phishing attempt.	- Deploy **email filtering solutions**. - Conduct **phishing awareness training**.	**Immediate (5-15 mins)** for detection. **30-60 mins** for containment. **1-2 hours** for eradication. **2-4 hours** for recovery.
DDoS Attack (Distributed Denial of Service)	- **AWS Shield**, **Cloudflare**: DDoS protection. - **Splunk**: Traffic analysis. - **Akamai**: Traffic monitoring.	- Engage DDoS protection. - Implement **rate-limiting**. - Apply **geo-blocking** if necessary.	- Re-route traffic to alternative regions. - Monitor for ongoing attack using **CloudWatch**. - Post-incident forensic analysis.	- Set up **load balancing**. - Implement **scalable infrastructure** with **Cloudflare/AWS Shield** protection.	**Immediate (5-15 mins)** for detection. **30-60 mins** for containment. **1-2 hours** for eradication. **4-12 hours** for recovery.

5.2 Incident Response Phases and Timeline

Phase	Action	Timeframe	Responsible Party
Detection	Initial detection through monitoring and alerting tools.	**Immediate (5-15 mins)**	SOC Analysts
Triage	Incident classification based on severity (Critical, High, Medium, Low).	**15-30 minutes**	Incident Response Lead, SOC Analysts

Phase	Action	Timeframe	Responsible Party
Containment	Isolate affected systems to limit the spread.	**30-60 minutes**	IT Engineers, SOC Analysts
Eradication	Remove the root cause (e.g., malware, unauthorized access).	**1-4 hours**	IT Engineers, Security Analysts
Recovery	Restore systems from backups or alternate environments.	**4-12 hours**	IT Support, Business Continuity
Post-Incident Review	Review the incident to improve future response processes.	**24-48 hours post-resolution**	Incident Response Lead, CISO

5.3 Detailed Incident Scenarios with Timelines

1. Unauthorized Access (Brute Force / Credential Stuffing)

Detection:

- **Okta** detects multiple failed login attempts within a short time frame.
- **CrowdStrike** identifies unusual access patterns (e.g., login from an unfamiliar country).

Actions:

- Lock the affected account and perform a **password reset**.
- Isolate the systems and restrict access to sensitive resources.
- Trigger **MFA** to prevent further unauthorized access.

Timeline:

- **Detection**: **Immediate (5-15 mins)**
- **Containment**: **30-60 mins**
- **Eradication**: **1-2 hours** (root cause analysis and remediation)
- **Recovery**: **4-12 hours** (restore and monitor)

Pre-Incident Planning:

- Enforce **MFA** for all critical systems.
- Implement **account lockout policies** after repeated failed login attempts.

---

2. Malware Infection (Ransomware)

Detection:

- **CrowdStrike Falcon** detects malware signatures or unusual file activity.
- **Splunk** correlates abnormal network traffic indicative of a data breach.

Actions:

- Immediately isolate the infected machine from the network.

- Run **antivirus scans** or use **CrowdStrike Falcon** for malware detection.
- Block all outbound communication to prevent further exfiltration of data.

Timeline:

- **Detection**: **Immediate (5-15 mins)**
- **Containment**: **30-60 mins**
- **Eradication**: **1-4 hours** (removal of malware and remediation)
- **Recovery**: **4-12 hours** (reimage systems and restore data)

Pre-Incident Planning:

- Deploy **ATP** on all devices.
- Maintain **offline backups** for critical systems.

---

3. Phishing Attack

Detection:

- **Mimecast** flags malicious email attachments or links.
- **Proofpoint** detects known phishing sites or unusual email behavior.

Actions:

- Quarantine the phishing email to prevent it from spreading.
- Perform **password reset** for all affected accounts.
- Trigger a **security sweep** of affected devices.

Timeline:

- **Detection**: **Immediate (5-15 mins)**
- **Containment**: **30-60 mins**
- **Eradication**: **1-2 hours** (removal of malicious links or files)
- **Recovery**: **2-4 hours** (restoration of email services and review of security settings)

Pre-Incident Planning:

- Deploy **email filtering solutions** for phishing detection.
- Conduct **phishing awareness training** to prevent user error.

---

4. DDoS Attack

Detection:

- **AWS Shield** detects traffic spikes that are typical of a DDoS attack.
- **Akamai** or **Cloudflare** identify abnormal traffic patterns or HTTP request anomalies.

Actions:

- Engage DDoS mitigation services such as **AWS Shield** or **Cloudflare** to absorb traffic.
- Implement **rate-limiting** and **geo-blocking** to prevent attack amplification.

- Re-route traffic to backup servers or use **load balancing** to mitigate strain on primary systems.

Timeline:

- **Detection**: **Immediate (5-15 mins)**
- **Containment**: **30-60 mins** (Activate DDoS protection, rate-limiting)
- **Eradication**: **1-2 hours** (traffic management and filtering)
- **Recovery**: **4-12 hours** (restore access and normal service)

Pre-Incident Planning:

- Use **load balancing** to distribute network traffic evenly.
- Implement **scalable cloud infrastructure** that can handle traffic spikes.

5.4 Communication Plan with Timelines

Action	Description	Responsible Party	Timeline
Internal Notification	Notify senior management, CISO, and incident response teams.	SOC Lead, Incident Response Lead	**Immediate (0-15 mins)**
External Notification	Notify affected users, clients, and regulatory bodies as required (e.g., GDPR breach notification).	PR Team, Legal, Incident Response Lead	**Within 1 hour of containment**
Public Disclosure	Announce any public-facing issues (only if necessary).	CISO, PR Team	**Post-resolution**
Stakeholder Updates	Provide regular updates to stakeholders (including impacted users) until resolution.	Incident Response Lead, CISO	**Ongoing (every 1-2 hours)**
Post-Incident Reporting	Document the full timeline and actions taken, including any failures and improvements.	Incident Response Lead, CISO	**Within 24-48 hours**

5.5 Post-Incident Review

Action	Description	Responsible Party	Timeline
Incident Report	Create a detailed incident report outlining what occurred, how it was handled, and its impact.	Incident Response Lead, CISO	**Within 24 hours**
Lessons Learned Session	Conduct a meeting with all relevant stakeholders to review the incident and derive improvement actions.	CISO, Incident Response Lead	**Within 48 hours**
Update Response Procedures	Revise the incident response plan based on lessons learned.	Incident Response Lead	**Within 72 hours**

Action	Description	Responsible Party	Timeline
Follow-up Training	Conduct refresher training and simulations for employees on the improved security protocols.	HR, Security Team	**Ongoing**

6. Data Backup, Recovery, and Business Continuity

6.1 Backup Strategy: The 3-2-1 Rule

Backup Components:

Backup Component	Description	Tools/Systems Used	Real-World Implementation	Pre-Incident Planning	Response Timeline
3 Copies of Data	Maintain three copies of data: the primary (live) copy, one backup copy stored locally, and one offsite backup copy.	- **Primary Data**: Live systems. - **Backup Copy 1**: Onsite backup with **Veeam Backup**. - **Backup Copy 2**: Offsite backup with **AWS S3** or **Azure Blob Storage**.	**Primary Copy**: Live systems, including production environments such as **SAP**, **Salesforce**, **Microsoft 365**, and critical operational data. **Backup Copy 1**: **Veeam Backup** on onsite **NAS (NetApp)** located in **UNICEF Geneva Data Center (Switzerland)**. **Backup Copy 2**: Cloud storage in **AWS S3** and **Azure Blob Storage** (Ireland for Europe and Singapore for Asia-Pacific).	- Backup jobs set up with **hourly** frequency for critical systems (e.g., payroll, financials, and HR systems). - **Cloud Storage** setup to include **geo-redundancy**.	**Backup Frequency**: **Hourly** for all critical systems. - **Backup Integrity Checks**: **Weekly** for onsite backups (NAS) and **monthly** for cloud backups (AWS S3, Azure Blob).

Backup Component	Description	Tools/Systems Used	Real-World Implementation	Pre-Incident Planning	Response Timeline
2 Different Media	Use two different types of media to ensure redundancy in case one medium fails.	- **Onsite Backup**: **NAS (Network Attached Storage)** for local storage. - **Offsite Backup**: Cloud storage (e.g., **AWS S3** or **Azure Blob Storage**).	**Onsite Backup**: 10 TB capacity **NetApp NAS** device in **Geneva (Switzerland)**, connected to internal systems. **Offsite Backup**: **AWS S3** in **EU-Ireland** and **Asia-Pacific-Singapore**, with backup data replicated between multiple regions for disaster recovery.	- Onsite NAS devices are **mirrored** to ensure **redundancy** within the Geneva data center. - **Cloud backup replication** ensures data in **Ireland** and **Singapore** is up-to-date with the latest hourly backup.	**Backup Frequency**: **Hourly** updates. - **Cloud Backup Verification**: Monthly verification tests using AWS and Azure to ensure data availability and integrity.
1 Offsite Location	Store at least one backup copy offsite, preferably in geographically separate locations to mitigate regional disasters.	- **Offsite Backup**: Cloud storage on **AWS S3** or **Azure Blob Storage**.	**Offsite Backup**: **AWS S3** in **Ireland (EU)** for European operations, **Singapore** region for Asia-Pacific. Use **AWS S3's geo-redundancy** to replicate backups across different availability zones and regions for resilience.	- Ensure **geo-redundant cloud storage** is configured to ensure backup copies are geographically separated. - **Automatic failover** mechanisms in place to restore operations from the secondary location.	**Backup Frequency**: **Hourly**. - **Disaster Recovery Simulation**: Annual simulation of cloud failover process for geo-redundancy validation.

Detailed Real-World Implementation of Backup Strategy:

- **Backup Frequency**:
  Critical systems are backed up hourly. This includes:
  - **Financial systems (SAP)**
  - **HR systems (Workday, payroll databases)**

    - **Client relationship management (Salesforce)**
    - **UNICEF core infrastructure data** These backups are performed with **Veeam Backup & Replication**, storing the data on **NetApp NAS** onsite and **AWS S3** offsite.

- **Backup Testing and Integrity**:
  Backups undergo verification every week to ensure consistency. If any issues are found, they are immediately addressed, and the most recent successful backup is restored to ensure readiness in case of disaster.

6.2 Recovery Point Objective (RPO) & Recovery Time Objective (RTO)

Recovery Point Objective (RPO)

RPO defines how much data loss is acceptable in the event of an incident, specifying how often backups should occur. For UNICEF, the **RPO is 1 hour**, meaning that data backups must happen at least every hour to ensure that, in the worst-case scenario, no more than one hour of data will be lost during a failure.

Metric	Value	Description	Tools/Systems Used	Real-World Implementation	Response Timeline
RPO	**1 hour**	Maximum allowable data loss during an incident (data loss is limited to one hour's worth of data).	- **Veeam Backup** (hourly onsite backups). - **AWS S3** (hourly offsite backups).	**Backup Frequency**: Data is backed up every **hour** for critical systems using **Veeam Backup** (on-premises) and **AWS S3** (cloud). All backups are validated and verified for integrity to ensure accurate restoration.	**Backup Frequency**: **Hourly**. **Backup Verification**: Weekly for on-premises backups and monthly for cloud backups.

RPO Real-World Implementation:

- **Automated Backups**:
  Critical systems like **SAP** and **Salesforce** are automatically backed up on an hourly basis. This minimizes the risk of data loss, ensuring that the most recent backup contains up-to-date records.

- **Incremental Backup Strategy**:
  To improve efficiency, only changes to data (incremental backups) are saved after the initial full backup, reducing backup time and storage requirements.

Recovery Time Objective (RTO)

RTO refers to the maximum time allowed for restoring systems and data after a disruption. UNICEF's **RTO is 4 hours**, meaning that the organization aims to restore critical services and data within **4 hours** of a disruption.

Metric	Value	Description	Tools/Systems Used	Real-World Implementation	Response Timeline
RTO	**4 hours**	Maximum allowable downtime for critical systems (systems must be operational within 4 hours).	- **Veeam Backup**: Onsite backup restoration. - **AWS S3**: Cloud-based restoration.	**Critical Systems Restoration**: Restoration of essential systems (e.g., **SAP**, **Salesforce**, **Workday**) must be completed within 4 hours. Backup systems are restored from **Veeam Backup** (onsite) or **AWS S3** (cloud) as required.	**Restoration Time**: Within **4 hours** for core systems.

RTO Real-World Implementation:

- **Prioritized Recovery**:
  SAP (ERP), **Salesforce** (CRM), and **Workday** (HR) are top priorities for restoration. These systems are critical to UNICEF's daily operations. After an incident, these systems must be restored first, within 4 hours of detection.
- **Redundancy for Critical Systems**:
  Redundant systems are in place to ensure these applications are available within the recovery window. For instance, **SAP** is backed up both onsite and in the cloud (via **AWS S3**), allowing for flexible restoration.

6.3 Business Continuity Planning (BCP)

BCP ensures UNICEF can continue essential functions during and after an incident. Here is how UNICEF has implemented its BCP:

BCP Component	Description	Tools/Systems Used	Real-World Implementation	Pre-Incident Planning	Response Timeline
Critical System Identification	Identify critical systems for prioritization in recovery.	- **SAP**, **Salesforce**, **Veeam Backup**, **AWS S3**	**Critical Systems**: **Salesforce**, **SAP**, **Workday** are listed as most critical. They are restored first, followed by secondary systems like email servers and internal collaboration tools.	- **Business Continuity Plan** prioritizes the **critical systems**. - Each critical application has a designated recovery owner.	**Immediate Identification**: 0-15 minutes after incident detection.

BCP Component	Description	Tools/Systems Used	Real-World Implementation	Pre-Incident Planning	Response Timeline
Alternate Site Activation	Establish alternate cloud environments to ensure continuity during an outage.	- **AWS EC2**, **Microsoft Azure**	Failover occurs to **AWS EC2** (Ireland) or **Azure** (Singapore) for critical services. If the Geneva data center becomes unavailable, cloud failover is automatically triggered.	- Cloud failover settings and **alternate site configurations** are pre-established. Cloud-based applications (e.g., Salesforce) are continuously mirrored.	**Immediate Failover Activation (within 1 hour)** if primary systems are down.
Data Access & Communication	Ensure employees can securely access critical data remotely and communicate during an incident.	- **Microsoft Teams**, **Slack**, **AWS WorkDocs**	**Microsoft Teams** and **Slack** serve as collaboration tools. Remote access is enabled via **VPN** for secure data access. **AWS WorkDocs** is used for document sharing in case of local system failures.	- Pre-configured **VPNs** for remote staff. **Cloud Collaboration** tools like **Microsoft Teams** and **Slack** are regularly tested.	**Immediate Communication Access**: Within **30 minutes** after failure.

6.4 Business Continuity Testing & Timeline

Action	Description	Responsible Party	Timeline
Backup Verification	Test backup systems regularly to verify data integrity and restore processes.	IT Support, Incident Response Lead	**Weekly for onsite backups**. **Monthly for cloud backups**
Disaster Recovery Drills	Full-scale recovery tests to simulate different disaster scenarios and ensure that the RTO is met.	IT Support, CISO	**Quarterly**

Action	Description	Responsible Party	Timeline
Business Continuity Test	Test business continuity protocols for critical systems, including systems failover to alternate locations.	Incident Response Lead, CISO	**Annually**
Post-Incident Review & Lessons Learned	After an incident, perform a review to identify areas for improvement and ensure continuous readiness.	Incident Response Lead, CISO	**Within 48 hours of incident resolution**

7. Endpoint Security

UNICEF's endpoint security strategy is essential to safeguard all devices used by employees, contractors, and remote staff. This includes desktops, laptops, mobile devices, and other types of endpoints. The purpose of this policy is to ensure that all endpoints are protected against security threats, vulnerabilities, and unauthorized access, minimizing the risk of data breaches and ensuring compliance with organizational and legal security requirements.

7.1 Tools for Endpoint Protection

UNICEF deploys a comprehensive suite of tools for endpoint protection, providing a layered defense strategy to protect against evolving cybersecurity threats. These tools are implemented globally across all UNICEF locations to ensure uniform security standards are maintained.

Security Tool	Description	Implementation	Deployment Locations
CrowdStrike Falcon	An advanced endpoint protection platform offering real-time threat detection, automated response, and incident investigation.	All devices are monitored continuously for potential security risks such as malware, ransomware, and APTs.	**All UNICEF offices and field locations worldwide** including **Geneva**, **Bangkok**, **New York**, **Bangladesh**, **South Sudan**.
Microsoft Defender for Endpoint	Provides comprehensive protection for **Windows**-based endpoints against malware, ransomware, and exploits.	Defender offers real-time protection, vulnerability management, and automated remediation for all Windows devices.	**Windows laptops and desktops** across all UNICEF locations.
VMware AirWatch (MDM)	A Mobile Device Management solution that manages and secures mobile devices like smartphones and tablets used by employees.	Enforces security policies such as device encryption, app whitelisting, and remote wipe in case of theft or loss.	Deployed on all mobile devices globally, especially for field workers in regions like **Uganda**, **Mexico**, **Afghanistan**, **Syria**.

Security Tool	Description	Implementation	Deployment Locations
Sophos Antivirus	A solution providing advanced protection against malware, ransomware, and other malicious activities on macOS devices.	Provides real-time detection of threats on macOS-based endpoints.	Implemented across all **macOS devices** used by staff in **Europe**, **Asia**, and **Americas**.
BitLocker (Windows)	Full disk encryption software for **Windows** laptops and desktops to protect data stored on the device in case of theft or unauthorized access.	Automatically encrypts all devices to ensure that sensitive information remains secure.	Applied to all **Windows laptops** and desktops across **global operations**.
FileVault (macOS)	Full disk encryption for **macOS** devices ensuring that all data is encrypted and protected against unauthorized access.	Applied to all **macOS** laptops and tablets used by staff and field personnel.	Applied globally, especially for field operations in **Syria**, **Lebanon**, and **South Sudan**.
AppLocker (Windows)	Application whitelisting tool that controls which applications can be executed on **Windows** devices, minimizing the risk of unapproved applications or malware.	Configured to block unauthorized applications from running on all **Windows** devices.	Enforced on all **Windows laptops** and **desktops** in **Europe**, **Africa**, and **Americas**.
Veeam Backup & Replication	Data backup solution ensuring that all endpoint data is backed up regularly to a secure offsite location, enabling rapid recovery in case of data loss or device failure.	Regular backups of endpoint data to ensure quick recovery in the event of an incident.	Deployed across **UNICEF offices** and **field locations**, with an emphasis on **Africa**, **Asia**, and **Middle East**.
Splunk Enterprise	Centralized log management and SIEM (Security Information and Event Management) platform used to monitor endpoint activities and identify potential security threats.	Aggregates security logs from endpoints across all locations for threat analysis, anomaly detection, and audit purposes.	Applied globally across all **UNICEF offices** and **remote field operations**.

7.2 Endpoint Protection Policy

UNICEF enforces a strict **Endpoint Protection Policy** that ensures all devices adhere to predefined security standards. This policy applies to all employees, contractors, and remote staff using any endpoint to access UNICEF's network, data, and systems.

Policy Component	Policy Details	Enforcement Mechanisms	Implementation Locations

Policy Component	Policy Details	Enforcement Mechanisms	Implementation Locations
Antivirus and Anti-malware	All endpoints must have antivirus and anti-malware software installed, configured, and updated regularly.	**Windows Defender** (for **Windows**), **Sophos Antivirus** (for **macOS**), **CrowdStrike Falcon** (for all devices).	Enforced globally across **Windows**, **macOS**, and mobile devices in **New York**, **Geneva**, **Bangladesh**, **Syria**, and other field offices.
Automatic Updates	Antivirus software must be set to automatically update to receive real-time protection against new and emerging threats.	Managed via **Centralized Management Systems** like **Splunk** and **CrowdStrike**. Automated updates are scheduled daily.	Ensured across all **UNICEF offices** and **remote locations** in **Africa**, **Asia**, **Americas**.
Full Disk Encryption (FDE)	All devices must use full disk encryption to ensure data is protected from unauthorized access in case of loss or theft.	**BitLocker** (for **Windows**) and **FileVault** (for **macOS**) are required and enforced on all devices.	Applied to all **Windows laptops**, **macOS laptops**, and **field devices** globally, especially for staff in **Africa** and **Middle East**.
Password Policy	Strong password policies are enforced on all devices to prevent unauthorized access to endpoints. Minimum complexity and periodic changes are required.	**Okta** for centralized authentication and **Active Directory** for enforcing password strength and change policies.	Enforced globally for all **UNICEF employees** across all locations.
Application Whitelisting	Only approved applications are allowed to run on devices to reduce the risk of malware or unauthorized software execution.	**AppLocker** for **Windows** and **Mobile Application Management** via **AirWatch**.	Applied to all **Windows laptops** and **mobile devices** across **Europe**, **Middle East**, **Asia**, **Africa**, and **Americas**.
Mobile Device Management (MDM)	All mobile devices used to access **UNICEF** systems must be managed by an MDM system to enforce security policies such as encryption, app whitelisting, and remote wipe.	Managed via **VMware AirWatch**, which enforces security settings for mobile devices.	Enforced globally for all mobile devices in **South Sudan**, **Lebanon**, **Pakistan**, and **Mexico**.

Policy Component	Policy Details	Enforcement Mechanisms	Implementation Locations
Remote Wipe	In case of loss or theft, devices must be remotely wiped to ensure that sensitive data is not exposed.	**Remote wipe** policies are integrated into **AirWatch**, **BitLocker**, and **FileVault** for mobile and non-mobile devices.	Globally enforced, especially in **high-risk** regions like **Syria**, **South Sudan**, **Uganda**, and **Honduras**.
Incident Reporting	Any suspicious activity or security incident must be immediately reported to the Security Operations Center (SOC) via the **ServiceNow** platform.	**SOC** responds to incidents with immediate investigation and remediation, using tools like **Splunk** and **CrowdStrike**.	Enforced across **all offices** in **New York**, **Geneva**, **Bangladesh**, **South Sudan**, **Syria**, **Mexico**, and **Lebanon**.

7.3 Monitoring and Response

UNICEF employs continuous endpoint monitoring, utilizing advanced detection technologies and centralized incident management systems to ensure rapid response to potential security incidents. Monitoring and response are crucial in maintaining endpoint security, particularly in detecting and mitigating any threats that may compromise the integrity of sensitive data.

Monitoring Tool	Description	Purpose	Response Mechanism
Splunk	Centralized log management and SIEM (Security Information and Event Management) platform for real-time endpoint monitoring.	Provides a global view of endpoint activity, detecting threats and suspicious behavior across all devices.	Immediate alerts for suspicious activity. Security teams are notified and an investigation is initiated.
CrowdStrike Falcon	Endpoint detection and response (EDR) tool for real-time threat monitoring and automated response.	Monitors all endpoints for threats like malware, unauthorized access, and system vulnerabilities.	Automated quarantine of infected devices. Incident response teams take action based on severity.
VMware AirWatch	Mobile device management tool that provides real-time monitoring of mobile devices and enforces security policies.	Detects and reports security incidents involving mobile devices.	Automated alerts triggered for non-compliant devices. Remote wipe or lockdown is applied if needed.
Microsoft Defender for Endpoint	Provides comprehensive threat and vulnerability management for Windows devices, including detection and remediation capabilities.	Detects and remediates threats on **Windows**-based endpoints.	Immediate detection and automated isolation of compromised endpoints. Follow-up investigation and remediation.

Monitoring Tool	Description	Purpose	Response Mechanism
Endpoint Detection and Response (EDR)	Integrated toolset combining **CrowdStrike**, **Microsoft Defender**, and **Splunk** to monitor, detect, and respond to security incidents across all endpoints.	Combines real-time monitoring, threat analysis, and automated response to ensure endpoints are protected.	Devices are isolated, threat source is identified, and remediation actions are applied.

By deploying these tools and enforcing the policies outlined above, UNICEF maintains a secure environment for all endpoints and ensures that all employees, contractors, and field staff adhere to the organization's cybersecurity standards.

---

8. Network Security & Cloud Protection

Overview

UNICEF's **Network Security & Cloud Protection** strategy is integral to safeguarding its critical digital infrastructure, ensuring that the organization can safely manage sensitive information and operate globally without disruption. With the increasing reliance on cloud services and a decentralized network of staff and partners, the implementation of advanced network and cloud security tools is crucial. The following outlines the network security measures and cloud protection tools deployed across UNICEF's infrastructure.

8.1 Network Security Tools

The core objective of network security is to ensure that UNICEF's internal network and digital assets are protected against unauthorized access, data breaches, and advanced persistent threats (APTs). UNICEF employs a multi-layered approach to network defense that integrates advanced technologies such as firewalls, intrusion detection systems, VPN solutions, and AI-powered network analysis.

1. Palo Alto Networks NGFW (Next-Generation Firewall)

Palo Alto Networks NGFWs are deployed at all perimeter network points across UNICEF's global offices and data centers, including **headquarters**, **regional offices**, and **cloud environments**. These firewalls protect against external and internal threats, offering application-level security and integration with global threat intelligence feeds.

- **Key Features**:
    - **Deep Packet Inspection (DPI)**: Analyzes incoming and outgoing traffic at the application layer to prevent attacks like **SQL injection**, **cross-site scripting (XSS)**, and other web application attacks.
    - **Threat Intelligence**: Integrates real-time threat intelligence feeds to block access to malicious IP addresses, domains, and URLs associated with known threats (e.g., ransomware, phishing).
    - **SSL Decryption**: Ensures that encrypted traffic (SSL/TLS) is inspected for hidden threats, ensuring end-to-end security.
- **Deployment**:
    - **Global Coverage**: Deployed across **UNICEF's data centers** in **New York (US East)**, **Brussels (Europe)**, **Singapore (APAC)**, **Kenya (Africa)**, and **Sydney (Australia)**.

    - **Cloud Environments**: Integrated with AWS and **Azure** cloud services, securing **VPCs (Virtual Private Clouds)** and protecting internal applications deployed across multiple regions.

2. Snort IDS/IPS (Intrusion Detection/Prevention System)

Snort serves as UNICEF's primary Intrusion Detection and Prevention System (IDS/IPS) to detect and block suspicious traffic based on predefined signatures. It analyzes both internal and external network traffic, providing **real-time monitoring** and threat detection.

- **Key Features**:
    - **Signature-Based Detection**: Detects known attack patterns such as **buffer overflows**, **brute-force login attempts**, and **zero-day exploits**.
    - **Protocol Analysis**: Ensures that protocols like **HTTP**, **FTP**, **SMTP**, and others are used securely and free from exploits.
    - **Alerting**: Sends real-time alerts to the **Security Operations Center (SOC)**, enabling rapid investigation and response.
- **Deployment**:
    - Installed across critical internal network segments, including employee workstations, data servers, and cloud environments, spanning **North America**, **Europe**, and **Africa**.
    - Deployed in both **UNICEF's on-premises** and **cloud infrastructure** to monitor internal network traffic in **AWS** and **Microsoft Azure**.

3. Palo Alto Networks VPN (GlobalProtect)

Palo Alto Networks GlobalProtect provides secure remote access for UNICEF's employees, contractors, and field staff operating worldwide. The VPN solution ensures that sensitive data remains encrypted while in transit, and that unauthorized users cannot access the internal network.

- **Key Features**:
    - **SSL Encryption**: Uses **SSL/TLS encryption** to secure data exchanges over the internet and prevent unauthorized interception.
    - **Multi-Factor Authentication (MFA)**: Ensures that only authorized personnel can access internal resources by requiring additional authentication factors.
    - **Client-Side Security**: Devices must meet security criteria (e.g., updated antivirus, encryption) before granting access to the network.
- **Deployment**:
    - VPN clients are deployed globally, with **priority for remote offices** and field operations in regions like **South Sudan**, **Syria**, and **Brazil** where internet security is crucial.
    - Also used by corporate employees and administrative teams accessing internal applications and files remotely from offices in **New York**, **London**, **Geneva**, and others.

4. Darktrace AI for Network Traffic Analysis

Darktrace is an AI-driven solution deployed to analyze and monitor network activity across all levels of the organization. It uses **machine learning** to continuously adapt to changes in network behavior and identify

potential security threats that may otherwise go undetected by traditional methods.

- **Key Features**:
    - **Anomaly Detection**: Detects unusual patterns of activity that indicate a potential breach, such as **lateral movement** within the network or unusual access to sensitive data.
    - **Self-Learning Capability**: Continuously learns and adapts to normal network behavior, reducing false positives and enabling more accurate threat detection.
    - **Autonomous Response**: Can take automated actions, such as quarantining suspicious devices or blocking traffic associated with malicious activity.
- **Deployment**:
    - Deployed globally, spanning all UNICEF offices, cloud environments, and external partner networks. Critical in regions with high-risk exposure to cyber threats like **East Africa** and **South America**.

8.2 Cloud Security

Given UNICEF's use of cloud platforms like **AWS**, **Microsoft Azure**, and **Google Cloud**, securing these environments is paramount. The following tools and strategies ensure data protection, compliance, and threat mitigation within cloud-based systems.

1. Prisma Cloud by Palo Alto Networks

Prisma Cloud provides end-to-end security for workloads across UNICEF's cloud environments, including **AWS**, **Azure**, and **Google Cloud**. The platform ensures compliance with global data protection regulations, such as **GDPR**, and scans cloud environments for vulnerabilities and misconfigurations.

- **Key Features**:
    - **Cloud Security Posture Management (CSPM)**: Continuously monitors cloud environments for misconfigurations, ensuring that resources are securely configured and compliant.
    - **Vulnerability Scanning**: Scans containers, virtual machines (VMs), and other resources for known vulnerabilities.
    - **Compliance Monitoring**: Assesses cloud configurations against frameworks like **ISO 27001**, **NIST**, and **GDPR** to ensure compliance with security standards.
- **Deployment**:
    - Implemented in UNICEF's **AWS** (Ireland, Singapore, US East), **Microsoft Azure** (Europe, North America), and **Google Cloud** platforms where the organization's critical data resides.
    - Specifically monitors **cloud-native applications**, **serverless functions**, and **data storage** (e.g., **S3 buckets**, **Azure Blob Storage**) to detect unauthorized access or data leakage.

2. Netskope CASB (Cloud Access Security Broker)

Netskope provides visibility and control over cloud applications, ensuring that data stored in SaaS platforms like **Google Workspace**, **Salesforce**, and **Dropbox** is accessed securely. It helps prevent **data leaks** and enforces **data loss prevention (DLP)** policies.

- **Key Features**:

    - **Real-Time Data Access Control**: Monitors all data interactions with cloud apps to ensure sensitive data isn't exposed or downloaded to unauthorized users.
    - **Shadow IT Discovery**: Identifies unauthorized cloud applications (Shadow IT) used by employees and partners to store or share sensitive information.
    - **Threat Protection**: Detects and prevents malware, ransomware, and phishing attempts in cloud environments.

- **Deployment**:

    - Deployed across **SaaS applications** used by UNICEF globally, such as **Google Workspace** (Docs, Sheets), **Dropbox**, and **Salesforce** for CRM and donor management.
    - Covers the organization's **global presence**, including high-risk areas like **Eastern Europe**, **Latin America**, and **South-East Asia**.

3. AWS CloudTrail

AWS CloudTrail is used to log every API call made within AWS services, ensuring visibility over all interactions with the cloud environment. CloudTrail provides detailed records of **who accessed what resources**, **when**, and **what actions were performed**.

- **Key Features**:

    - **API Activity Logging**: Captures every action made in AWS, including who initiated the request, what was changed, and the outcome.
    - **Audit Trails**: Helps forensic teams investigate suspicious activities and provides evidence for compliance audits.
    - **Multi-Region Support**: Ensures CloudTrail logs are collected and stored in multiple regions to avoid data loss in case of a regional service outage.

- **Deployment**:

    - Active across all UNICEF **AWS regions** including **Ireland**, **Singapore**, and **US East** where sensitive data like donor information, financial records, and program data are stored.
    - Ensures that logs are available for security audits, helping UNICEF maintain compliance with global regulations such as **GDPR** and **FISMA**.

4. Azure Security Center

Azure Security Center offers a unified infrastructure security management system that provides threat protection across Microsoft Azure. It assists UNICEF in monitoring and managing security policies across their Azure resources to prevent unauthorized access, data breaches, and configuration drift.

- **Key Features**:

    - **Regulatory Compliance Monitoring**: Continuously assesses security configurations against standards such as **ISO 27001**, **NIST** guidelines, and **GDPR** to ensure that resources remain compliant.
    - **Threat Detection and Mitigation**: Integrates with other Azure services like **Azure Sentinel** to detect vulnerabilities, malware, and **advanced persistent threats (APTs)**.

- **Deployment**:

- Implemented in all UNICEF **Azure cloud services** supporting mission-critical operations, including personnel data management systems, **SAP applications**, and financial management platforms hosted in **Germany**, **North America**, and **Asia-Pacific**.

Incident Response for Network & Cloud Security

UNICEF's incident response plan for network and cloud security is structured to quickly identify, contain, and mitigate potential security breaches. The process ensures that each incident is swiftly dealt with,

minimizing damage and ensuring compliance with data protection regulations.

Phase	Action	Timeframe	Responsible Party
Detection	Alerts from **Palo Alto NGFW**, **Snort**, and **Prisma Cloud** signal potential security breaches.	Immediate (within minutes)	SOC Team, Security Analysts
Triage	Assessing the scope and potential impact of the incident, prioritizing response efforts based on severity.	10-30 minutes	Incident Response Lead, SOC Team
Containment	Isolating compromised systems or cloud resources using **firewalls** and **security groups**.	30-60 minutes	IT Operations, Security Analysts
Eradication	Identifying malicious processes or unauthorized users and removing them from the environment.	1-2 hours	IT Support, Security Analysts
Recovery	Restoring services from backups (e.g., **AWS S3**, **Azure Recovery**) and verifying systems are secure.	2-4 hours	IT Support, Cloud Infrastructure Teams
Post-Incident Review	Root cause analysis, impact assessment, and lessons learned to improve future response and prevention.	24-48 hours post-resolution	CISO, Incident Response Lead

---

9. Employee Awareness and Training

9.1 Security Awareness Training

UNICEF's employee awareness and training programs are designed to continuously improve the security culture within the organization. Training focuses on practical scenarios and critical cyber threats, with a strong emphasis on hands-on testing through simulated exercises.

Training Platforms and Tools

1. **KnowBe4**:
    - **Training and Phishing Simulation Platform**: UNICEF uses **KnowBe4** as the primary platform for delivering training content and conducting phishing simulations. This platform offers interactive training modules on a wide range of cybersecurity topics.

- **Phishing Simulation Tool**: **KnowBe4** sends simulated phishing emails to employees to assess their ability to recognize malicious emails. These emails are tailored to reflect real-world attack vectors relevant to UNICEF's operations.

2. **Cybersecurity Awareness Hub**:

   - **Internal Knowledge Base**: In addition to **KnowBe4**, UNICEF maintains an internal hub for security resources, which includes guides, FAQs, and video tutorials on handling data securely, avoiding social engineering, and using internal tools (like **Slack**, **Workday**, and **Salesforce**) securely.
   - **Mandatory Security Refresher Training**: On a quarterly basis, all employees must revisit core security concepts through mandatory refresher training courses, which include reviewing recent phishing attack patterns, cybersecurity tips, and best practices for data handling.

Training Topics

1. **Phishing and Social Engineering**:

   - **Objective**: Equip employees with the skills to recognize common phishing attempts and social engineering tactics designed to steal sensitive data.
   - **Training Duration**: 1.5 hours (initial) / 30-minute refresher (quarterly).
   - **Delivery**: Online interactive course with real-world phishing email simulations.
   - **Example**: Employees will encounter a simulated phishing email purporting to be from UNICEF's HR department requesting them to click a link to verify their bank details. The training provides tips on identifying such emails, including suspicious links and spelling errors.

2. **Data Protection and Secure Handling**:

   - **Objective**: Ensure that employees understand the importance of data protection, how to store and share sensitive information securely, and how to comply with regulations such as GDPR and UNICEF's internal privacy policies.
   - **Training Duration**: 1 hour.
   - **Frequency**: Annual.
   - **Example**: Training includes guidelines on using **Microsoft Teams** for secure messaging, encryption of sensitive data using **PGP** (Pretty Good Privacy), and how to use **SharePoint** and **OneDrive** securely to store files.

3. **Password Management**:

   - **Objective**: Encourage employees to use strong passwords and multi-factor authentication (MFA) to protect their accounts.
   - **Training Duration**: 45 minutes.
   - **Frequency**: Annual.
   - **Example**: Employees are shown how to use **LastPass** to generate and store complex passwords and how to configure MFA for essential systems like **Workday** and **SAP**. The training also includes a segment on the dangers of password reuse and tips on creating passphrases.

4. **Mobile Device Security**:

   - **Objective**: Educate employees on securing mobile devices, including smartphones, laptops, and tablets, particularly for those working in remote and field environments.
   - **Training Duration**: 1 hour.

- **Frequency**: Annual (with an optional quarterly reminder).
- **Example**: Instructions on using **VMware AirWatch** for device management, enforcing full disk encryption, setting up VPNs, and configuring remote wipe for lost or stolen devices.

5. **Incident Reporting and Response**:

   - **Objective**: Provide employees with a clear understanding of how to report security incidents, and their role in the organization's broader incident response plan.
   - **Training Duration**: 45 minutes.
   - **Frequency**: Bi-annual.
   - **Example**: Employees are trained to recognize potential security incidents such as data breaches, phishing emails, and unauthorized access attempts, and are provided with specific guidelines on reporting incidents via the **ServiceNow** platform.

9.2 Phishing Simulations and Testing

UNICEF leverages **KnowBe4** to conduct monthly phishing simulations to assess employees' abilities to identify phishing attempts. These simulations are specifically designed to mimic real-world attack tactics and test the overall readiness of employees.

Phishing Simulation Process

1. **Monthly Campaigns**:

   - **Customization**: Each phishing simulation is custom-built to reflect current cyber threats and specific UNICEF environments (e.g., focusing on emails claiming to be from UNICEF donors or partners).
   - **Types of Attacks**:
     - **Spear Phishing**: Personalized emails targeting specific individuals or departments, such as finance, with requests to process urgent payments.
     - **Whaling**: High-level phishing attacks targeting senior executives, often impersonating other executives or senior staff members.
     - **Credential Harvesting**: Simulated emails asking employees to click on a link and log in to a fake **Workday** or **Salesforce** login page to steal credentials.

2. **Real-Time Monitoring and Feedback**:

   - **Immediate Feedback**: When an employee clicks on a phishing link or submits personal information, they receive immediate feedback from **KnowBe4**, which includes a brief training session to educate them on how to spot phishing attacks.
   - **Targeted Follow-up Training**: Employees who repeatedly fall for phishing simulations are enrolled in additional, targeted training sessions focused on phishing and social engineering.

3. **Reporting and Tracking**:

   - **Monthly Reports**: At the end of each simulation campaign, the results are aggregated into detailed reports showing how many employees clicked on malicious links, how quickly they reported the phishing attempt, and which employees require additional training.
   - **Trend Analysis**: Reports allow UNICEF's security team to identify trends over time. For instance, if a specific department is consistently targeted or a particular attack vector is successful, additional

training sessions will be scheduled.

9.3 Role-Based and Specialized Training

Certain roles within UNICEF, such as IT staff, system administrators, and senior management, require specialized, in-depth cybersecurity training. These training programs focus on advanced threats and operational security responsibilities.

Role-Specific Training Programs

1. **IT Administrators and System Engineers**:
    - **Training Focus**: Advanced network security techniques, vulnerability assessments, patch management, incident response protocols, and secure system configuration.
    - **Tools Covered**: **Splunk**, **CrowdStrike**, **Palo Alto Networks**, and **AWS CloudTrail**.
    - **Frequency**: Quarterly.
    - **Duration**: 3 hours per session.
2. **Security Team and Incident Response Personnel**:
    - **Training Focus**: Incident response procedures, digital forensics, managing a breach, and coordination with law enforcement if needed.
    - **Frequency**: Quarterly simulations, such as tabletop exercises, and real-world incident response drills.
    - **Duration**: 4-5 hours per session.
3. **Senior Management and Executives**:
    - **Training Focus**: Understanding security risks at an enterprise level, securing business-critical data, and supporting cybersecurity strategies.
    - **Topics**: Crisis management during data breaches, executive-level communication, and cyber risk management.
    - **Frequency**: Annual.
    - **Duration**: 2 hours per session.

9.4 Training Schedule and Timeline

To ensure that employees receive regular and relevant cybersecurity training, UNICEF adheres to the following **Training and Awareness Timeline**. This schedule is integrated into the employees' annual development plans, with mandatory participation for all relevant staff.

Month	Activity	Target Audience	Duration	Frequency
January	**New Year Security Awareness Kick-off**	All employees	1 hour	Annual
February	**Phishing Simulation**	All employees	15 minutes	Monthly

Month	Activity	Target Audience	Duration	Frequency
March	**Password Management and MFA Training**	All employees	1 hour	Annual
April	**Security Training for IT/Admins**	IT staff, system administrators	3 hours	Quarterly
May	**Mobile Device Security**	Remote workers, field staff	1 hour	Annual
June	**Data Protection & Handling of Sensitive Information**	All employees	1.5 hours	Annual
July	**Incident Response Training** (Simulated Incident Response)	Security team, incident responders	4 hours	Quarterly
August	**Phishing Simulation**	All employees	15 minutes	Monthly
September	**Advanced Security for Executives**	Executives, senior management	2 hours	Annual
October	**Security Essentials for Remote Workers**	Remote workers, field staff	1 hour	Annual
November	**Phishing Simulation**	All employees	15 minutes	Monthly
December	**End-of-Year Security Review and Awareness**	All employees	1 hour	Annual

9.5 Measuring Training Effectiveness

Training effectiveness is assessed using multiple metrics to ensure the security program evolves and meets its objectives.

1

. **Phishing Click Rates**: Monitor how often employees click on phishing links in monthly simulations. Over time, these rates should decline, indicating that the workforce is becoming more vigilant. 2. **Knowledge Assessments**: Quizzes at the end of training sessions assess employee comprehension. Employees who score below a certain threshold are flagged for follow-up training. 3. **Incident Response Metrics**: Evaluate how well employees respond to actual security incidents, particularly in terms of timely reporting, adherence to procedures, and involvement in mitigation efforts. 4. **Security Awareness Culture Metrics**: Surveys and feedback from employees help gauge the effectiveness of the training programs and identify any areas that require improvement.

9.6 Continuous Improvement

The training program is always evolving based on feedback, industry trends, and emerging threats.

- **Quarterly Reviews**: Regular meetings with IT, HR, and the security team to review the latest phishing simulation results, incident reports, and training feedback.
- **Emerging Threats**: New training content is developed as new threats emerge, ensuring that employees are always equipped to defend against the latest attack methods.
- **Ongoing Feedback Loop**: Employees are encouraged to provide feedback on the training experience and suggest areas for improvement, ensuring that the training remains relevant, engaging, and effective.

Here's a **detailed, extended**, and **realistic** presentation of UNICEF's security measures for **Physical Security**, **Vendor and Third-Party Security**, **Security Audits and Monitoring**, and associated processes, complete with **actionable timelines** and **clear, structured** formatting.

---

10. Physical Security

UNICEF employs a comprehensive physical security strategy to safeguard its data, infrastructure, and personnel across its global operations. The approach includes advanced access control, surveillance, and environmental monitoring to ensure that critical facilities are secure from both internal and external threats.

10.1 Data Center Security

UNICEF's data centers are critical assets that host sensitive data and systems essential for the organization's operations worldwide. Protecting these assets from physical security threats, such as unauthorized access, theft, vandalism, and environmental hazards (e.g., fire, flooding), is paramount.

Security Measures:

- **Biometric Access Control**:
    - **Objective**: Ensure that only authorized personnel can access high-security areas within the data center, such as server rooms, network infrastructure, and other sensitive locations.
    - **Process**: UNICEF employs **biometric access controls** (e.g., **fingerprint scanners**, **retina scans**, and **facial recognition**) in all high-security areas within its data centers. These systems log every entry and exit, which is tracked and reviewed on a regular basis to ensure only authorized individuals have access.
    - **Timeline**: The biometric access systems undergo an **annual review** for efficiency and accuracy. Additionally, access permissions are updated **quarterly** to reflect changes in personnel roles and responsibilities. For example, IT personnel may have broader access privileges, which are updated as needed.
        - **Example**: At the **Geneva Data Center**, biometric systems ensure that only a select group of IT staff have access to the core infrastructure. Security personnel conduct monthly reviews of the logs to identify any irregularities or unauthorized access attempts, ensuring compliance with internal security protocols.
- **Surveillance Systems**:
    - **Objective**: Continuously monitor the premises to detect any unauthorized physical access or suspicious activity.

- **Process**: High-definition CCTV cameras are installed throughout the data centers, with both **daytime and infrared night-vision capabilities** for 24/7 monitoring. These cameras are integrated into an advanced **surveillance management system**, which provides **real-time alerts** for any unusual activities. The surveillance feeds are constantly monitored by the **Global Security Operations Center (GSOC)**, which is responsible for incident response coordination.

- **Timeline**: CCTV cameras are **inspected weekly** to ensure proper functionality. A **monthly maintenance cycle** is in place to calibrate the cameras and check for any system malfunctions. The system stores surveillance footage for **30 days**, after which it is archived for long-term retention. Any suspicious activity recorded is reviewed by security officers within **24 hours**.

    - **Example**: The **New York Data Center** is equipped with over **300 high-definition cameras**, with **motion sensors** that can detect movement in real-time. In the event of any suspicious movement, the system triggers an instant notification to the **security team**, who can take immediate action. Anomalies such as an attempt to bypass security gates or access restricted zones are flagged and escalated for further investigation.

- **Environmental Controls**:

    - **Objective**: Safeguard critical IT infrastructure from damage caused by environmental hazards, such as fire, flooding, and temperature fluctuations.

    - **Process**: All data centers are equipped with state-of-the-art **environmental controls**, including **fire suppression systems** (e.g., **Halon gas**), **flood detection sensors**, and **temperature and humidity controls** (HVAC systems). The fire suppression systems are designed to prevent the spread of fire without damaging sensitive electronic equipment. Regular **environmental hazard simulations** and **drills** are performed to ensure the systems operate as intended during emergencies.

    - **Timeline**: The environmental systems undergo **monthly diagnostic checks** by both internal teams and third-party contractors. In addition, **annual fire and flood safety audits** are performed to ensure compliance with safety regulations and operational readiness.

        - **Example**: In **Singapore**, the data center has **flood detection sensors** that immediately alert security teams if water levels rise beyond a certain threshold. In case of fire, the **Halon suppression system** is activated automatically. A routine diagnostic check is performed by an external contractor every **first Monday of the month** to ensure the entire infrastructure is fully operational.

10.2 Office Security

UNICEF’s office facilities are another crucial aspect of its physical security infrastructure. These offices house employees, contractors, and visitors, and it is imperative to maintain strict security protocols to protect both personnel and sensitive information.

Security Measures:

- **Smart Card Access**:

- **Objective**: To regulate and control access to secure areas within the office, ensuring that only authorized personnel can enter sensitive locations such as meeting rooms, laboratories, and server rooms.

- **Process**: UNICEF utilizes **smart card technology** for access control. Each employee, contractor, and visitor is issued a **smart card** that provides access to specific areas within the office. The smart cards are integrated with **PIN code authentication**, and each access attempt is logged. These logs are reviewed regularly by the security team to ensure compliance.

- **Timeline**: Access logs are reviewed on a **monthly basis**, and any discrepancies are escalated to the security team for immediate investigation. Additionally, **quarterly updates** are performed on the smart card system to ensure that access permissions reflect current employee roles and clearance levels.

    - **Example**: In **UNICEF's New York Headquarters**, the **main building, server rooms, and research laboratories** are all secured with smart card access. When an employee's role changes (e.g., promotion, transfer), their access privileges are updated within **24 hours** to ensure that only authorized personnel can access sensitive areas.

- **Visitor Management System**:

    - **Objective**: To ensure that all visitors to UNICEF offices are properly identified, tracked, and escorted in sensitive areas.

    - **Process**: All visitors are required to **register** at the reception desk upon arrival. They are asked to provide valid **photo identification** and indicate the purpose of their visit. Visitors are issued a **visitor badge** that is valid for the duration of their visit. Visitors accessing sensitive areas are assigned an employee escort, who ensures they remain in authorized zones.

    - **Timeline**: Visitor logs are reviewed **quarterly** to ensure the system is functioning efficiently. Any trends or security concerns (such as unauthorized access attempts or unescorted visits) are addressed immediately, and security protocols are adjusted accordingly.

        - **Example**: At **UNICEF's Geneva Office**, visitors to high-security areas like the research labs and data centers must wear **tracked visitor badges** and be accompanied by an employee at all times. The system also logs the exact time of entry and exit, providing a detailed history of all visits for security audits.

Summary and Continuous Improvement

UNICEF's **Physical Security** strategy is designed to protect its critical data and infrastructure from both internal and external threats. Through stringent access control, surveillance, and environmental monitoring, the organization ensures that all its facilities are secure and compliant with global security standards. Regular audits and reviews are performed to continuously improve the systems, and all security measures are integrated with **Global Security Operations Centers (GSOC)** to ensure real-time monitoring and incident response.

Timeline for Security Review and Improvements:

- **Monthly**: Surveillance systems check, smart card access audits, visitor log review.
- **Quarterly**: Access permissions updates, visitor system audit, security protocol adjustments.

- **Annually**: Comprehensive review of biometric systems, fire suppression systems, and vendor-provided environmental safety audits.

Here is an extended and more detailed version of the **Vendor and Third-Party Security** section, incorporating more comprehensive operational processes, timelines, and real-world examples:

---

11. Vendor and Third-Party Security

Given the critical nature of third-party services in supporting UNICEF's operations, ensuring the security and compliance of these external partners is vital. UNICEF adheres to rigorous vendor risk management practices and conducts thorough security assessments to mitigate risks associated with third-party vendors.

11.1 Vendor Risk Management

Before any vendor or third-party service is onboarded, UNICEF ensures that the vendor’s security posture meets or exceeds industry standards and complies with relevant regulations. This includes a comprehensive review of the vendor's data handling, security protocols, and legal compliance.

Security Evaluation and Onboarding:

- **Security Assessments**:
    - **Objective**: Ensure that vendors align with UNICEF's data protection policies, network security measures, and international regulatory requirements.
    - **Process**: All prospective vendors undergo an initial **security evaluation** before being onboarded. This evaluation covers a range of factors, including:
        - **Data Protection Policies**: Does the vendor have appropriate measures for data encryption, secure storage, and secure transmission of sensitive information?
        - **Compliance with Regulatory Standards**: Does the vendor comply with international laws like **GDPR**, **HIPAA**, and **ISO 27001** standards?
        - **Network Security Protocols**: Does the vendor implement effective firewalls, intrusion detection systems (IDS), and endpoint protection to secure their systems?
    - **Timeline**: The security evaluation process is typically completed **within 30 days** of initiating a vendor relationship. Following the onboarding, UNICEF performs **bi-annual reviews** to ensure ongoing compliance with security protocols.
        - **Example**: When selecting a **cloud storage provider**, UNICEF requires the vendor to submit a detailed report on their **data encryption standards**, including their use of **end-to-end encryption** and multi-factor authentication for accessing sensitive files. This report is reviewed by UNICEF's security team and external auditors, ensuring alignment with the **ISO 27001** compliance standard.
- **Data Protection and Compliance**:
    - **Objective**: To ensure that all vendors handle personal and sensitive data in compliance with global data protection laws.

- **Process**: All vendors are required to sign a **Data Processing Agreement (DPA)** that outlines the expectations for data handling, storage, and protection, particularly for **personally identifiable information (PII)**. Additionally, vendors are expected to provide **annual compliance assessments** or reports demonstrating adherence to data protection regulations such as **GDPR**, **HIPAA**, and **CCPA**.

- **Timeline**: The **DPA** is reviewed and signed during the contract negotiation phase, with **annual reviews** scheduled to coincide with the contract renewal period. Vendors are required to submit **quarterly security compliance reports**, ensuring they are continuously in line with regulatory requirements.

    - **Example**: UNICEF's **third-party cloud service provider** is required to undergo a **quarterly data protection audit**, focusing on data encryption, data retention policies, and user access controls. The vendor must submit an updated compliance report each quarter to confirm adherence to **GDPR** and data protection laws. Failure to comply with the audit requirements may result in a contract review or termination.

11.2 Third-Party Security Audits

Annual security audits are essential in verifying the vendor's adherence to UNICEF's stringent security policies. These audits, conducted by independent third-party organizations, evaluate vendors' internal controls, data protection measures, and compliance with industry standards.

Security Audits Process:

- **Annual Security Audits**:

    - **Objective**: To conduct a comprehensive review of the vendor's security posture, focusing on areas such as risk management, data encryption, access control, incident response, and vulnerability management.

    - **Process**: UNICEF employs reputable third-party auditors such as **KPMG**, **PwC**, and **Deloitte** to perform **annual security audits**. These audits assess the vendor's adherence to best practices in cybersecurity and data protection, including:

        - **Vulnerability Scanning**: Identifying potential weaknesses in the vendor's network infrastructure and system configurations.
        - **Compliance Verification**: Ensuring the vendor meets global regulatory standards (e.g., **ISO 27001**, **GDPR**, **NIST**).
        - **Incident Response Readiness**: Evaluating the vendor's ability to detect, respond to, and recover from security incidents, such as data breaches or system compromises.

    - **Timeline**: These audits are performed **annually**, with findings reported within **30 days** of the audit's completion. If a significant vulnerability or non-compliance issue is identified, follow-up audits are scheduled sooner.

        - **Example**: An **annual audit** of a **managed IT services vendor** may uncover several outdated software systems with known vulnerabilities. The audit team will provide a **30-day corrective action plan** for the vendor to address these issues and update their systems.

- **Follow-Up on Audit Findings**:
    - **Objective**: Ensure that any vulnerabilities or compliance failures identified during an audit are addressed promptly by the vendor to mitigate potential security risks.
    - **Process**: After each audit, UNICEF schedules a **follow-up meeting** with the vendor to discuss the findings and agree on a **corrective action plan (CAP)**. This plan outlines specific remediation steps, timelines for completion, and responsibilities assigned to both parties.
    - **Timeline**: Corrective actions for **critical vulnerabilities** (e.g., unpatched security flaws or unauthorized access) must be implemented **within 30 days**. For **non-critical findings**, such as minor procedural improvements, the vendor has up to **90 days** to implement the necessary changes. UNICEF monitors the progress of these actions through regular meetings and updates.
        - **Example**: Following an audit of an external **cloud storage vendor**, it was discovered that their access controls for certain data repositories were not adequately secured. UNICEF issued a **30-day corrective action plan**, requiring the vendor to enhance their encryption and implement more robust user authentication measures. The vendor successfully updated their protocols within the allotted timeframe.

11.3 Vendor Offboarding and Data Disposal

When a vendor relationship is terminated, UNICEF ensures that all vendor access is revoked and that sensitive data is securely returned or destroyed.

Security Measures:

- **Access Termination**: Upon the end of the vendor contract, all access credentials and accounts are immediately disabled, and any devices or systems provided to the vendor are returned or securely wiped.
- **Data Destruction**: All data stored by the vendor is either returned to UNICEF or securely destroyed, following industry best practices for **data sanitization**.
- **Timeline**: Data destruction occurs within **30 days** of contract termination, with a signed certificate from the vendor confirming the completion of the process.
    - **Example**: When UNICEF ends a contract with a **data analytics provider**, the vendor is required to submit a **Data Destruction Certificate** within **30 days**, confirming that all UNICEF data stored in their systems has been deleted and securely wiped from all devices.

Summary and Continuous Monitoring

The **Vendor and Third-Party Security** practices at UNICEF ensure that vendors meet rigorous standards for data protection, compliance, and risk management. By conducting **security assessments**, **audits**, and **ongoing monitoring**, UNICEF maintains a secure supply chain and ensures that sensitive data is protected at all stages of the vendor relationship.

Timeline for Vendor Security Management:

- **Initial Evaluation**: Completed within **30 days** of vendor engagement.

- **Bi-annual Vendor Review**: Conducted every **6 months**.
- **Annual Security Audits**: Performed once a year, with follow-up actions completed within **30-90 days** depending on the severity of the findings.
- **Offboarding and Data Disposal**: Finalized within **30 days** of contract termination.

---

12. Security Audits and Monitoring

12.1 Continuous Monitoring

Continuous monitoring is an essential component of UNICEF's cybersecurity strategy. It involves the real-time tracking of systems, network traffic, and endpoints to detect threats and respond promptly to security incidents. Monitoring tools are integral in ensuring that potential vulnerabilities or attacks are identified early, allowing for fast mitigation.

Monitoring Tools:

- **Splunk**:
    - **Objective**: Splunk serves as a **centralized log management** and **real-time analytics** platform for monitoring all critical systems and networks. The tool aggregates data from multiple sources, including servers, network devices, cloud platforms, firewalls, and endpoints, to provide detailed insights into the overall security posture.
    - **Process**: Data is collected, normalized, and analyzed to generate **real-time alerts** for anomalies that could signify potential threats, such as unauthorized access attempts, suspicious user activity, or configuration errors. This enables the **Security Operations Center (SOC)** to quickly identify and respond to security incidents.
    - **Timeline**: Continuous monitoring is active **24/7**, with monthly evaluations of the aggregation and alerting processes to ensure no gaps in data collection. The SOC team reviews security logs in real-time, with **monthly audits** conducted to ensure accuracy and completeness of data. Regular updates to monitoring rules and threat intelligence feeds are done **quarterly** to adapt to emerging threats.
        - **Key Actions**:
            - **Real-time alert generation** when unusual network activity or unauthorized logins are detected.
            - **Detailed analysis** and investigation of all incidents flagged by Splunk, enabling quick identification of potential breaches.
- **CrowdStrike Falcon**:
    - **Objective**: CrowdStrike provides **endpoint protection** through real-time monitoring of all devices, detecting malware, ransomware, and abnormal behaviors indicative of a cyber attack.
    - **Process**: The tool continuously monitors endpoints (servers, laptops, mobile devices, etc.) for unusual activities such as file modifications, unauthorized access to sensitive data, or the execution of known malware. Upon detection of any threat, CrowdStrike isolates the affected endpoint, preventing the spread of the threat and sending an alert to the SOC team.

    - **Timeline**: Monitoring runs **24/7**, with **weekly updates** and patching to ensure that endpoints are protected from the latest threats. The SOC team receives alerts in real-time, with daily reviews of the status of endpoints across the organization.

        - **Key Actions**:
            - **Malware or ransomware isolation**: When malicious activity is detected, CrowdStrike isolates the endpoint to prevent further spread.
            - **Real-time incident alerts** sent to the SOC, allowing immediate response to prevent damage.

- **Network Traffic Analysis Tools (e.g., Darktrace)**:

    - **Objective**: Darktrace utilizes **artificial intelligence (AI)** and machine learning to detect **anomalous network behaviors** that may indicate a cybersecurity threat, including data exfiltration, unauthorized lateral movement, or abnormal access patterns.

    - **Process**: Darktrace uses AI to establish a baseline of normal network traffic behavior. Once baseline patterns are established, it automatically detects deviations that may suggest an ongoing attack. The system sends alerts to the SOC when suspicious patterns are identified, such as unauthorized access to sensitive data, unusual outbound traffic, or attempts to bypass network security controls.

    - **Timeline**: Continuous, real-time monitoring is conducted, with **quarterly evaluations** of the threat detection capabilities and network traffic analysis policies. Regular updates to the AI models are made to keep up with emerging attack techniques.

        - **Key Actions**:
            - **AI-driven anomaly detection** to identify potential insider threats or compromised accounts.
            - **Real-time alerts** and notifications when abnormal traffic or suspicious activities are detected.

12.2 External Audits

External audits play a critical role in ensuring that UNICEF's security infrastructure complies with relevant regulations and global standards. These audits help ensure that the organization maintains high standards of security and aligns with best practices for risk management, data protection, and system controls.

Audit Process:

- **ISO 27001 and GDPR Compliance Audits**:

    - **Objective**: To assess the effectiveness of UNICEF's Information Security Management System (ISMS) in accordance with **ISO 27001** and verify adherence to global data protection laws, such as the **General Data Protection Regulation (GDPR)**.

    - **Process**: UNICEF engages independent third-party auditors to conduct comprehensive reviews of its security framework and data protection practices. The auditors assess various aspects, including:

        - **Risk Management Processes**: Evaluating how risks are identified, assessed, and mitigated across the organization.
        - **Data Protection Measures**: Reviewing data encryption, access controls, and GDPR compliance mechanisms.
        - **Incident Response Procedures**: Testing the readiness and effectiveness of response to data breaches or security incidents.
        - **Access Controls**: Ensuring that only authorized individuals can access sensitive data and systems.

    - **Timeline**: **Annual audits** are conducted, typically starting in **Q1**, with reports delivered within **30-45 days** of the audit's completion. The findings are used to inform corrective actions and process improvements. Any immediate issues are addressed and resolved within **30 days**.

        - **Key Actions**:
            - **ISO 27001 Audit**: Evaluating overall ISMS policies and controls to ensure they meet international standards.
            - **GDPR Compliance Check**: Reviewing practices to ensure that personal data is processed and protected in accordance with the regulation.
            - **Follow-up corrective actions**: Prompt implementation of any corrective actions identified during the audit.

- **Follow-Up on Audit Findings**:

    - **Objective**: To ensure that identified vulnerabilities or compliance issues are addressed promptly and effectively.

    - **Process**: After each audit, a follow-up meeting is held between UNICEF's security team, external auditors, and relevant stakeholders. A corrective action plan (CAP) is created to address the findings. UNICEF works closely with external auditors and internal teams to resolve issues quickly and efficiently.

    - **Timeline**: Corrective actions are typically completed within **30 days** for high-priority issues (e.g., security vulnerabilities or non-compliance with critical regulations). Less critical issues are addressed within **60-90 days**.

        - **Key Actions**:
            - **Immediate remediation** of high-priority vulnerabilities.
            - **Documentation of corrective actions** taken and verification that the issues have been resolved.
            - **Monitoring of progress** through follow-up meetings and internal audits.

- **ISO 27001 Surveillance Audits**:

    - **Objective**: To ensure that UNICEF's ISMS remains compliant with ISO 27001 standards and that security measures are continuously improved.
    - **Process**: ISO 27001 surveillance audits occur annually and assess the organization's ability to maintain and improve its ISMS. The audit includes a review of the effectiveness of risk management strategies, information handling practices, incident response procedures, and employee awareness of security protocols.
    - **Timeline**: These audits are conducted **annually**, and the organization is required to make improvements based on the audit's findings. The process typically starts in **Q2** with a follow-up

audit conducted at the end of the year to verify the implementation of corrective actions.

12.3 Incident Response and Audit Integration

Integrating security audits with incident response protocols is crucial for ensuring that security issues are resolved efficiently and that the organization learns from past incidents to improve its defenses.

Incident Management Integration:

- **Objective**: To ensure that audit findings and continuous monitoring tools support swift and effective incident response actions.
- **Process**: When a security incident is detected, the SOC team collaborates with IT, legal, and compliance teams to assess the scope of the incident. Audit results and data from monitoring tools like Splunk, CrowdStrike, and Darktrace are reviewed to understand how the breach occurred, what systems were affected, and how the response could be improved in the future.
- **Timeline**: Incident response begins immediately following the detection of a threat, with initial containment and analysis conducted within **minutes to hours** depending on the severity of the incident. Post-incident reviews are held **within 7 days** to assess the effectiveness of the response and integrate lessons learned into future security strategies.
    - **Key Actions**:
        - **Post-incident review** to identify gaps in security controls.
        - **Collaboration with external auditors** to evaluate incident impact and ensure that all audit findings are incorporated into the response plan.
        - **Improvement of incident response plans** based on audit feedback.

Summary and Timeline for Security Audits and Monitoring:

- **Continuous Monitoring** with tools like Splunk, CrowdStrike, and Darktrace is operational **24/7** with real-time alerts and weekly updates to maintain optimal system protection.
- **Annual Audits** (ISO 27001, GDPR, etc.) are completed by third-party auditors, typically delivered within **30-45 days** of audit completion, followed by immediate corrective actions if needed.
- **Post-Incident Reviews** are integrated with monitoring tools and audit feedback, and corrective actions are initiated **within 30 days** for critical issues and **90 days** for less severe findings.

---

13. Document Control and Review Cycle

To ensure the ongoing effectiveness and relevance of security policies, procedures, and controls, UNICEF employs a formal **Document Control and Review Cycle**. This cycle ensures that all security-related documentation is continually evaluated, updated, and maintained in alignment with evolving threats, regulatory requirements, and organizational changes.

13.1 Policy Review

The policy review process is central to ensuring that UNICEF's security policies stay up-to-date with current risks, legal standards, and best practices.

- **Objective**: To regularly assess and update security policies and practices in response to changing security threats, technological advancements, and regulatory requirements.
- **Timeline**: Security policies are reviewed on an **annual basis** to ensure they remain effective and relevant. In cases of a security breach or significant regulatory change, a policy review is triggered immediately, with updates being made within **30 days**.

Review Process:

1. **Annual Review**:
    - Each year, all security policies and guidelines are comprehensively reviewed. This ensures that all procedures reflect the latest best practices and comply with industry standards and legal requirements.
    - Any internal changes, such as system upgrades, policy amendments, or operational changes, are taken into account during the review.
2. **Post-Incident Review**:
    - If a security incident occurs, an immediate review of relevant policies is conducted to determine their effectiveness in mitigating the threat. Following the review, necessary updates are made to prevent future occurrences. These updates must be implemented within **30 days**.
3. **Ad-Hoc Reviews**:
    - In response to new emerging risks, regulatory changes, or technological advancements, policies may be reviewed outside the scheduled review cycle. These reviews are initiated promptly, with updates made within **30 days** of identification.

13.2 Document Control

Document control ensures that security policies, procedures, and related documents are properly maintained, updated, and stored in a secure, accessible manner.

- **Objective**: To ensure that all security documentation is version-controlled, securely stored, and accessible only to authorized personnel.
- **Process**:
    1. **Centralized Repository**: All security-related documents are stored in a centralized, secure repository. Access to this repository is strictly controlled, and only authorized personnel can modify or approve documents.
    2. **Version Control**: A strict version control mechanism is employed to ensure that historical versions of documents are preserved while only the latest version is actively used. Any changes to documents are tracked with detailed version history, including modification dates and reasons for changes.
    3. **Approval Process**: Before a document is finalized or updated, it must go through a formal approval process. This process ensures that relevant stakeholders, including security, legal, and compliance teams, review and approve the changes before they are adopted.
- **Timeline**:

- **Monthly Document Audits**: All security documents are audited on a monthly basis to ensure that they are up-to-date, relevant, and aligned with the latest regulations.
- **Quarterly Review Cycle**: In addition to monthly audits, a more comprehensive review of all security documents takes place quarterly. This process ensures that the documentation is comprehensive and aligns with the current security strategy.

13.3 Document Communication and Training

Effective communication and training ensure that all employees and relevant stakeholders understand and comply with updated security policies.

- **Objective**: To ensure that updates to security policies are effectively communicated to all relevant parties and that staff members are trained to implement new or revised security measures.
- **Process**:
  1. **Communication of Policy Changes**: All policy changes are communicated to employees and stakeholders via internal communications channels, such as email, intranet postings, or security bulletins. This ensures that everyone is informed of the updates and understands their responsibilities.
  2. **Training on Updated Policies**: Employees are required to complete training sessions on any new or updated policies. This ensures that all staff members are equipped with the knowledge and skills needed to adhere to the updated security measures.
  3. **Tracking Compliance**: Compliance with training requirements is tracked through a certification system. Records of training completion are stored and reviewed during audits to ensure that all relevant personnel are up to date on security protocols.
- **Timeline**:
  - **Bi-Annual Training**: Training on security policies is conducted at least twice a year. Additional training sessions are scheduled as needed following significant policy changes or security incidents.

13.4 Audit and Review of Compliance

To ensure that the document control process is being properly followed, regular audits and reviews of compliance are conducted.

- **Objective**: To verify that all security policies and documents are being reviewed, updated, and followed in accordance with internal procedures and external regulatory requirements.
- **Process**:
  1. **Internal Audits**: Internal audits are conducted regularly to evaluate adherence to document control procedures. These audits assess whether policies are being reviewed and updated according to established timelines, and if all necessary changes are being implemented.
  2. **Compliance Audits**: Annual compliance audits are performed to verify that the document control process aligns with regulatory requirements such as **ISO 27001**, **GDPR**, and other relevant standards. These audits also assess the effectiveness of the security documentation in meeting the organization's overall security goals.
- **Timeline**:

- **Internal Audits**: Conducted quarterly to ensure the effectiveness of the document control and review cycle.
- **Compliance Audits**: Conducted annually to assess compliance with industry standards and regulatory requirements.

13.5 Key Elements of the Document Control and Review Cycle

- **Regular Reviews**: Security policies are reviewed annually and updated as necessary. Immediate reviews occur following incidents or major regulatory changes.
- **Version Control**: Documents are maintained with strict version control to ensure traceability of changes.
- **Approval and Training**: Security policies undergo a formal approval process and are followed by training for all relevant stakeholders.
- **Compliance Audits**: Both internal and external audits ensure adherence to the document control process and overall compliance with security standards.

---

14. Continuous Improvement

Continuous improvement is a critical component of UNICEF's cybersecurity strategy. This process ensures that security measures are always evolving in response to emerging threats, new technological developments, and lessons learned from previous security incidents. UNICEF aims to maintain a proactive and adaptive security posture to safeguard its infrastructure, data, and operations.

14.1 Framework for Continuous Improvement

The continuous improvement framework follows a structured, multi-step approach to enhance security practices over time. This process is designed to address current security gaps, integrate new technologies, and ensure compliance with the latest standards and regulations.

Key Components:

- **Adaptation**: Responding to new security risks, threat actor tactics, and regulatory changes.
- **Efficiency**: Streamlining processes and eliminating inefficiencies in the detection, prevention, and response to threats.
- **Innovation**: Embracing advanced technologies and methodologies to stay ahead of evolving cyber threats.
- **Resilience**: Strengthening the organization's ability to prevent, detect, and recover from security incidents.

14.2 Security Feedback Loops

Security feedback loops are vital to the continuous improvement process. These loops capture insights from various sources, such as internal evaluations, incident reviews, employee feedback, and industry threat intelligence. They are integral in refining security policies, procedures, and tools.

Feedback Sources:

- **Incident Reviews**: Following any significant security incident, a post-mortem analysis is conducted to identify the root causes and areas for improvement in security practices. These findings directly inform security policy revisions.

    - **Timeline**: Post-incident reviews are held within **48 hours** of an event, and action plans for improvement are created within **30 days**.

- **Employee Feedback**: Regular surveys and internal discussions are used to gather feedback from staff on the effectiveness of security training programs, tools, and overall security awareness.

    - **Timeline**: Feedback is collected bi-annually, with immediate actions taken for urgent issues identified in surveys.

- **Threat Intelligence**: UNICEF leverages threat intelligence shared by external partners, government bodies, and industry groups to gain insights into emerging threats and tactics used by cybercriminals. This information is used to adjust internal security measures accordingly.

    - **Timeline**: Threat intelligence is continuously monitored and integrated into the organization's security framework.

14.3 Security Assessments and Audits

Regular security assessments and audits are essential for identifying vulnerabilities, measuring the effectiveness of current security measures, and ensuring compliance with industry regulations. These assessments help to identify gaps in security controls and provide a basis for prioritizing improvements.

Types of Security Assessments:

- **Vulnerability Scanning and Penetration Testing**: Regular vulnerability scans and penetration tests are conducted to simulate attacks and identify weaknesses in the system.

    - **Timeline**: Vulnerability assessments are carried out **quarterly**, with immediate remediation of critical issues identified. Penetration tests are conducted **annually** or after significant system changes.

- **Compliance Audits**: To ensure compliance with regulatory standards such as GDPR, ISO 27001, and other relevant frameworks, UNICEF undergoes regular internal and external audits.

    - **Timeline**: Compliance audits are conducted **annually**, with ongoing monitoring for continuous compliance throughout the year.

- **Third-Party Audits**: External security firms are hired to audit the security practices of third-party vendors and contractors, ensuring that they meet UNICEF's security and privacy standards.

    - **Timeline**: Third-party audits are conducted on a yearly basis, with follow-up assessments required if any security gaps are identified.

14.4 Technology Adoption and Integration

Adopting new technologies is a key strategy for improving UNICEF's security posture. Continuous evaluation of emerging tools and techniques ensures that the organization stays ahead of new threats and remains compliant with evolving regulations.

Key Areas of Focus:

- **Automation and Orchestration**: Automation of threat detection, incident response, and security workflows helps reduce human error, increase operational efficiency, and speed up response times.
    - **Timeline**: Automation technologies are evaluated for integration **every six months**. New automation tools are implemented based on effectiveness and organizational needs.
- **Artificial Intelligence (AI) and Machine Learning (ML)**: AI and ML are integrated into threat detection systems to improve accuracy and speed in identifying potential threats. These technologies help identify patterns that would be difficult for human analysts to spot.
    - **Timeline**: AI and ML tools are reviewed for integration **quarterly**, with continuous training of these systems to improve detection capabilities.
- **Next-Generation Security Tools**: UNICEF regularly reviews its use of next-generation firewalls, endpoint protection, and network monitoring tools. The goal is to ensure that the latest tools, which incorporate advanced threat intelligence and behavioral analytics, are used to secure the organization.
    - **Timeline**: A review of security tools and systems takes place **bi-annually**, and updates are scheduled based on threat landscape changes and technological advancements.

14.5 Employee Training and Awareness

Employee awareness is a critical element of UNICEF's continuous improvement strategy. As the human element is often the weakest link in cybersecurity, continuous training and awareness programs are designed to ensure that employees are prepared to recognize and respond to potential threats.

Training Programs:

- **Ongoing Security Training**: All employees undergo security awareness training that is updated regularly to reflect the latest threats and best practices. This includes training on phishing, password management, secure data handling, and incident reporting.
    - **Timeline**: Security training is conducted **quarterly**, with mandatory refresher courses for employees who have not completed training within the last six months.
- **Phishing Simulations**: Simulated phishing attacks are conducted regularly to test employee awareness and preparedness in identifying phishing attempts. Results from these simulations guide further training improvements.
    - **Timeline**: Phishing simulations are conducted **bi-annually**, with targeted follow-up training provided to employees who fail the tests.
- **Security Champions Program**: Certain employees are designated as security champions within their teams. These champions promote security best practices, encourage awareness, and act as a liaison between their teams and the security department.
    - **Timeline**: Security champions are selected **annually**, with periodic check-ins and assessments on their effectiveness in promoting security within their teams.

14.6 Key Performance Indicators (KPIs)

To measure the effectiveness of continuous improvement efforts, UNICEF uses Key Performance Indicators (KPIs). These KPIs help track progress, identify areas for improvement, and evaluate the impact of changes made to security protocols and tools.

Key KPIs Include:

- **Incident Detection Time**: The average time taken to detect a security incident from the point of occurrence.
- **Response Time**: The time taken to contain and resolve a security incident once detected.
- **Vulnerability Remediation Rate**: The percentage of identified vulnerabilities that are addressed within specified timeframes.
- **Training Effectiveness**: Measured by the completion rate of training sessions and the success rate in phishing simulations.
- **Compliance Status**: The level of compliance with internal security policies, as well as external regulations (e.g., GDPR, ISO 27001).

14.7 Reporting and Documentation

All continuous improvement efforts are documented to maintain accountability and provide transparency to both internal and external stakeholders. Regular reports on the progress of improvement initiatives, audit findings, training activities, and vulnerability management are shared with senior management, and when necessary, with external auditors.

Documentation:

- **Quarterly Reports**: Detailed reports on the status of ongoing security improvement initiatives, including assessments, audits, and incident response metrics.
    - **Timeline**: Reports are submitted **quarterly**, with a comprehensive annual review summarizing the year’s activities, improvements, and results.
- **Annual Security Review**: A comprehensive review of the organization’s security posture, including the effectiveness of policies, technologies, and training programs, as well as the organization’s response to new threats and regulatory changes.
    - **Timeline**: The annual security review is completed **at the end of each fiscal year**, with a focus on setting goals for the following year.

14.8 Governance and Oversight

The continuous improvement process is overseen by UNICEF’s senior leadership, with regular updates provided to the board and relevant stakeholders. This ensures that security remains a priority at all levels of the organization and that resources are allocated to improve security controls.

Governance:

- **Security Steering Committee**: A cross-functional committee consisting of senior leadership, IT security, legal, compliance, and other relevant departments meets regularly to review security performance and guide improvement efforts.

- **Timeline**: The Security Steering Committee meets **quarterly** to review progress and adjust the organization's security strategy as needed.

---

15. Emerging Threats and Future Security Trends

UNICEF is committed to staying ahead of evolving security challenges to protect its sensitive data, infrastructure, and operations. This forward-looking approach involves preparing for emerging threats and adopting cutting-edge technologies that can help mitigate risks and enhance overall cybersecurity resilience.

15.1 Ransomware and Data Protection

Ransomware remains one of the most significant cyber threats to organizations worldwide, including those in humanitarian and international development sectors like UNICEF. As cybercriminals develop more sophisticated ransomware strains, it is essential to strengthen defenses and response capabilities.

Ransomware Mitigation Strategies:

- **Backup Strategies**: UNICEF continuously enhances its backup strategies to ensure that critical data is securely stored and can be quickly restored in the event of a ransomware attack. Regular **backup testing** is conducted to verify recovery procedures and ensure data integrity.
  - **Timeline**: Backup systems are tested quarterly, and full restoration exercises are conducted **annually** to validate data recovery processes.
- **Endpoint Protection**: Using advanced **endpoint protection tools**, such as **CrowdStrike Falcon**, UNICEF works to prevent ransomware from reaching endpoints through behavior analysis, anomaly detection, and real-time response.
  - **Timeline**: Endpoint protection tools are continuously updated with the latest threat intelligence to stay ahead of evolving ransomware tactics. Monthly updates are conducted for signature databases and detection rules.
- **Incident Response Plans**: To minimize the impact of ransomware attacks, UNICEF's **Incident Response (IR) plan** incorporates detailed procedures for containment, communication, and recovery. The plan is tested and updated regularly.
  - **Timeline**: The IR plan is reviewed and updated **annually**. Ransomware-specific response simulations and tabletop exercises are conducted bi-annually.
- **Employee Training**: Phishing remains a primary vector for ransomware infections, so continuous security awareness and phishing simulations are conducted to ensure employees are prepared to identify suspicious emails.
  - **Timeline**: Phishing awareness training is carried out quarterly, and simulated phishing attacks are executed **bi-annually** to evaluate employee readiness.

15.2 Artificial Intelligence and Machine Learning in Security

Artificial Intelligence (AI) and Machine Learning (ML) are playing an increasingly important role in cybersecurity by improving the detection and response to security threats. These technologies can help UNICEF identify emerging threats, predict potential vulnerabilities, and automate responses to incidents.

AI and ML Integration:

- **Threat Detection and Analytics**: UNICEF is investing in AI/ML technologies to improve the detection of advanced persistent threats (APTs), insider threats, and zero-day vulnerabilities. By analyzing large volumes of data, AI systems can identify patterns and anomalies that might go unnoticed by traditional systems.
    - **Timeline**: AI/ML tools are continuously evaluated and refined to adapt to new threats. A comprehensive evaluation of AI-based threat detection tools is conducted **annually**.
- **Behavioral Analytics**: Machine learning algorithms are used to monitor the behavior of users and devices across the network, creating baseline profiles. Any deviation from the baseline can trigger alerts, enabling faster identification of potential threats.
    - **Timeline**: Behavioral analytics tools are updated and calibrated **quarterly** to enhance detection accuracy and minimize false positives.
- **Automated Incident Response**: AI/ML is also used to automate certain aspects of the incident response process, such as blocking malicious traffic, isolating compromised systems, and applying security patches. This reduces response time and helps contain threats more effectively.
    - **Timeline**: Automated response processes are evaluated every six months, with updates implemented as necessary based on new threat intelligence.

15.3 Zero Trust Architecture (ZTA)

As organizations continue to face evolving security risks, the traditional perimeter-based security model is becoming increasingly ineffective. UNICEF is transitioning to a **Zero Trust Architecture (ZTA)**, which assumes that no user or device, whether inside or outside the network, can be trusted by default.

Zero Trust Implementation:

- **Identity and Access Management (IAM)**: The foundation of ZTA is the principle of least privilege, meaning that users only have access to the specific resources they need to perform their tasks. **Multi-factor authentication (MFA)** and strict **access controls** are applied to all users, devices, and applications.
    - **Timeline**: ZTA implementation is ongoing. MFA is required for all critical systems, with periodic audits of access controls conducted every 6 months to ensure compliance with the Zero Trust model.
- **Micro-Segmentation**: To prevent lateral movement in the event of a breach, UNICEF is implementing **micro-segmentation** across its network. This involves segmenting the network into smaller, isolated parts, so that even if one segment is compromised, the attacker is unable to move freely across the entire network.
    - **Timeline**: Network segmentation and ZTA deployment is phased, with significant progress expected by the end of **2025**. Key milestones include completing the implementation of micro-segmentation in critical network zones within **12 months**.
- **Continuous Authentication and Monitoring**: In a Zero Trust environment, authentication is continuous, and all traffic is monitored for unusual behavior. This includes evaluating the trustworthiness of devices

and users at every stage of interaction, regardless of their location.

- **Timeline**: Continuous authentication mechanisms are being rolled out incrementally, with initial deployment expected in **Q2 2025**. Ongoing monitoring and adjustments are made as the system matures.

15.4 Cloud Security and the Shift to Cloud-First

As more services and applications move to the cloud, securing cloud environments is a growing priority. UNICEF's strategy includes adopting a **cloud-first approach**, while ensuring that cloud services meet rigorous security standards and comply with relevant data protection regulations.

Cloud Security Measures:

- **Cloud Access Security Brokers (CASBs)**: UNICEF utilizes **CASBs** to monitor and control data movement across various cloud platforms, ensuring that data access is properly governed, and that security policies are enforced consistently.
  - **Timeline**: CASB solutions are deployed across all major cloud platforms by **mid-2025**, with ongoing monitoring and adjustment based on evolving security needs.
- **Cloud Encryption**: All sensitive data stored in the cloud is encrypted both in transit and at rest. Encryption keys are managed through a secure system to prevent unauthorized access.
  - **Timeline**: Cloud encryption strategies are reviewed **annually** to ensure they align with evolving encryption standards and compliance requirements.
- **Vendor Risk Management**: As UNICEF continues to engage with third-party cloud service providers, vendor risk management practices ensure that these providers comply with security standards, data protection regulations, and internal policies.
  - **Timeline**: Vendor security audits are conducted **annually**, with additional assessments triggered after any major contract updates or cloud service changes.

15.5 Threat Intelligence Sharing and Collaboration

In the face of rapidly evolving threats, cybersecurity is becoming increasingly collaborative. UNICEF actively participates in information-sharing initiatives and collaborates with other organizations, industry leaders, and government entities to exchange threat intelligence.

Collaboration Efforts:

- **Public-Private Partnerships**: UNICEF collaborates with government agencies, non-governmental organizations (NGOs), and private-sector cybersecurity firms to stay informed about new threats and to share best practices.
  - **Timeline**: Partnerships are reviewed and refreshed **annually**, with regular exchanges of threat intelligence conducted as new information becomes available.
- **Industry Groups and Forums**: UNICEF is an active member of various cybersecurity forums and industry groups, where threat intelligence is shared, and joint defense measures are discussed.

    - **Timeline**: Participation in industry groups occurs on an ongoing basis, with quarterly updates on threat intelligence and new cyber defense techniques.

15.6 Artificial Intelligence and Autonomous Security Systems

As part of its forward-looking strategy, UNICEF is exploring the use of **autonomous security systems** powered by AI to proactively monitor, detect, and respond to cyber threats without direct human intervention. These systems will use machine learning algorithms to analyze vast amounts of network data and make security decisions in real-time.

Implementation Plans:

- **AI-Driven Threat Detection**: Advanced machine learning models will be developed to detect new, unknown types of cyber threats by analyzing network traffic patterns, user behaviors, and system anomalies.
    - **Timeline**: The pilot phase of AI-driven threat detection is expected to begin in **late 2025**, with full deployment scheduled for **2027**.
- **Autonomous Response Systems**: As AI technologies mature, UNICEF plans to integrate autonomous security response capabilities, where the system can take action (e.g., blocking malicious traffic, isolating infected endpoints) without requiring manual intervention.
    - **Timeline**: Full deployment of autonomous response systems is targeted for **2027**, with gradual implementation starting in **2026**.

15.7 Quantum Computing and Post-Quantum Cryptography

Quantum computing is expected to revolutionize the field of cybersecurity, with both the potential to break current encryption schemes and the ability to offer stronger encryption models. UNICEF is actively monitoring developments in **post-quantum cryptography (PQC)**, ensuring that it is prepared to transition to quantum-resistant cryptographic methods.

PQC Strategy:

- **Monitoring Quantum Advances**: UNICEF is tracking developments in quantum computing and post-quantum cryptography to anticipate the need for a shift to quantum-safe encryption protocols.
    - **Timeline**: A formal strategy for transitioning to post-quantum cryptography is being developed, with initial research and preparation scheduled for **2026**.