IT Protection and Security: MIT 264
Alden A. Quiñones
Activity 9: Security Policy Development

ICT PROTECTION AND SECURITY POLICY FOR THE DEPARTMENT OF SOCIAL WELFARE AND DEVELOPMENT (DSWD) FIELD OFFICE XII

RATIONALE:

The DSWD Field Office XII is committed to ensuring the protection and integrity of its IT infrastructure, data, and systems by implementing robust security measures. This policy establishes clear standards and best practices for the secure management, operation, and access control of all computer units, software applications, internal systems, and network resources. These measures are designed to safeguard sensitive information, uphold data confidentiality, ensure data integrity, and guarantee the continuous availability of critical services. By enforcing these guidelines, the DSWD Field Office XII aims to mitigate security risks, comply with legal and regulatory requirements, and foster a secure environment that supports the efficient and safe delivery of services to the public. This policy not only outlines essential security protocols but also emphasizes the importance of a culture of security awareness and responsibility across all levels of the organization.

OBJECTIVE:

The objective of this policy is to:

- Ensure the secure management of IT resources and data within the DSWD Field Office XII.
- Protect sensitive information from unauthorized access, alteration, or destruction.
- Maintain compliance with relevant laws, regulations, and internal standards.
- Ensure that all IT assets, applications, and systems are protected from security risks and vulnerabilities.

SCOPE:

This policy applies to:

- All employees, contractors, and third-party vendors who interact with or manage IT resources, systems, and data within the DSWD Field Office XII.
- All computer units (desktop PCs, laptops, and mobile devices) connected to the DSWD Field Office XII network.
- All software applications, both internal and third-party, used by DSWD Field Office XII.
- All internally developed application systems and their deployment.
- All network systems, including VPN access and firewall security.
- All IT-related concerns raised through the ICT Support System.

REFERENCE

This policy is supported by and aligned with the following:

- **Republic Act No. 10173** – Data Privacy Act of 2012

IT Protection and Security: MIT 264
Alden A. Quiñones
Activity 9: Security Policy Development

- **Republic Act No. 8792** – Electronic Commerce Act of 2000
- **ISO/IEC 27001** – Information Security Management Systems (ISMS)
- **NIST SP 800-53** – Security and Privacy Controls for Federal Information Systems and Organizations
- **OWASP Top 10** – Web Application Security Risks
- **DSWD Administrative Order No. 10** – Guidelines for Information Technology Systems Security and Data Management
- **COA Guidelines** – Commission on Audit Guidelines for Disposal of Assets

DEFINITION OF TERMS

- **Confidentiality**: Ensuring that sensitive data is accessible only to authorized individuals.
- **Integrity**: Protecting data from unauthorized changes to ensure its accuracy and reliability.
- **Availability**: Ensuring that data and IT systems are accessible when needed by authorized users.
- **Access Control**: Restricting system access to authorized users based on their roles and responsibilities.
- **End-point Protection**: Protecting devices (computers, laptops, etc.) from security threats using software like PaloAlto XDR.
- **TLS (Transport Layer Security)**: A cryptographic protocol designed to protect data transmitted over a network.
- **Incident Response**: The process of responding to and managing security incidents, including breaches or attacks.

GUIDELINES

1. **Computer Units**

    - All computer units must be registered to the **ENTDSWD.LOCAL** domain controller.
    - All computer units designated for disposal must be properly documented, including the Certificate of Acceptance (COA), and must comply with COA guidelines.
    - All computer units issued to employees who are exiting the organization (due to termination, retirement, or resignation) should be surrendered to the ICTMS.
    - All computer units must have PaloAlto XDR installed as endpoint protection to detect and prevent threats.
    - All computer units must be regularly audited for compliance with security policies, including checks for unauthorized software or hardware modifications.
    - Any computer unit that experiences security breaches or operational issues must be reported immediately to the ICTMS for further investigation and resolution.
    - Computer units must be equipped with up-to-date antivirus software and undergo regular scans to detect and eliminate potential threats.
    - All computer units must be configured with strong password policies and multi-factor authentication (MFA) enabled where applicable.
    - Computer units that are deemed outdated or unable to meet current security and operational standards must be replaced or upgraded in coordination with the ICTMS.

2. **Software Applications**

- Only whitelisted software applications are allowed.
- Any software installation requests must be submitted to the ICTMS with proper justification.
- All installed software must be regularly updated to ensure security patches are applied promptly.
- Unauthorized software installations or use of unapproved software will be subject to disciplinary action.
- Software applications that are no longer in use or have reached their end-of-life must be uninstalled and removed from the system.
- Software applications must comply with all relevant licensing agreements and intellectual property laws.

3. **Access & Security**

- All access outside the DSWD VPN should be restricted. Only users with valid **GlobalProtect** credentials issued by the ICTMS are authorized for remote access.
- All accounts (Active Directory, corporate emails, and application accounts) must adhere to a strict password policy. Passwords should contain at least 8 characters, including a mix of upper and lower case letters, numbers, and special characters, and must be changed every 90 days.
- Multi-factor authentication (MFA) must be enabled for all accounts, especially for those with access to sensitive or critical systems.
- User access rights must be regularly reviewed and adjusted based on the principle of least privilege, ensuring that users only have access to resources necessary for their job functions.
- All access attempts and activities must be logged and monitored to detect any unauthorized or suspicious behavior.
- User accounts that are inactive for more than 30 days should be disabled, and any accounts associated with terminated employees must be promptly deactivated by the ICTMS.
- All devices used for remote access must comply with security standards, including updated antivirus software and endpoint protection mechanisms.
- Any unauthorized access attempts or security incidents should be immediately reported to ICTMS and investigated for potential vulnerabilities.
- Access to critical systems must be secured using encryption, ensuring that sensitive data is protected during transmission.
- Access to administrative privileges must be restricted and granted only to authorized personnel with documented approval from management.

4. **Internally Developed Application Systems**

- All internally developed applications must undergo a vulnerability assessment before receiving deployment authorization.
- All internally developed web-based application systems must use **TLS 1.3** or later for secure data transmission.

- All code for internally developed applications must undergo a thorough code review to identify potential security flaws, inefficiencies, or vulnerabilities.
- Developers must adhere to secure coding practices, including input validation, output encoding, and avoiding hard-coded credentials, to minimize the risk of exploitation.
- All internally developed applications must undergo comprehensive testing, including functional, security, and performance testing, to ensure they meet the organization's standards before deployment.
- Any security vulnerabilities identified in deployed internally developed applications must be patched promptly, with updates tested and deployed according to the organization's patch management policy.
- Internally developed applications must have strict access control mechanisms in place to ensure that only authorized users can access sensitive data or perform critical functions.
- In the event of a security incident involving an internally developed application, a formal incident response plan must be followed to contain, assess, and resolve the issue in accordance with security protocols.
- All internally developed applications must include logging and monitoring mechanisms to track user activities and detect any abnormal behavior or potential security threats.
- Detailed documentation for all internally developed applications must be maintained, including system architecture, data flows, and security measures, to assist in ongoing maintenance, troubleshooting, and security assessments.

5. **ICT Support**

- All ICT-related issues or concerns should be raised to the ICT Support System via ictsupport.fo12@dswd.gov.ph.
- All support requests will be acknowledged within 24 hours, and a resolution or update will be provided within the agreed-upon time frame, depending on the priority level of the issue.
- Support requests will be categorized based on severity, with critical issues (e.g., system outages, data breaches) receiving immediate attention, and non-urgent issues (e.g., minor software glitches) addressed within a standard time frame.
- If an issue cannot be resolved within the designated response time, it will be escalated to the appropriate level of support or management for further action.
- All support requests, resolutions, and actions taken must be documented for future reference and troubleshooting.
- The ICT Support team will offer regular training sessions and user guides to ensure all employees are equipped to handle common ICT-related issues and understand basic troubleshooting steps.
- All hardware and software assets requiring support will be tracked in the ICT asset management system, ensuring proper documentation for repairs, replacements, and upgrades.
- After resolution, the ICT Support team will conduct a follow-up to ensure that the issue has been fully resolved and that no further issues are arising from the same request.
- Remote support tools will be used, where applicable, to provide efficient troubleshooting and resolution without requiring on-site visits.

- The ICT Support team will adhere to the established SLA for response and resolution times, ensuring consistent and reliable service for all users.

6. **Security Measures**

1. All IT systems must implement **role-based access control (RBAC)** to ensure users only have access to the data and systems necessary for their roles.
2. Employees must use strong passwords, as described above, and ensure that passwords are changed every 90 days.
3. All sensitive data, whether in transit or at rest, must be encrypted using industry-standard encryption protocols (e.g., AES, TLS).
4. Sensitive data should only be retained as long as necessary for business and legal purposes and must be securely disposed of when no longer needed.
5. Firewalls, intrusion detection systems (IDS), and other security measures should be used to protect the network from unauthorized access.
6. All security incidents must be reported immediately to ICTMS. A designated incident response team will address and mitigate risks related to security breaches.
7. All employees and contractors must participate in regular cybersecurity training to understand the importance of data protection and the risks of security threats.
8. Any third-party vendors must comply with DSWD security standards and undergo a security assessment before being granted access to organizational systems or data.

ADMINISTRATION

- The **ICTMS (Information and Communications Technology Management Service)** is responsible for the implementation, monitoring, enforcement, and review of this policy.

a. **ICTMS Head:**

- Oversee the implementation, enforcement, and continuous improvement of the ICT policies.
- Lead the review of the policy on an annual basis to ensure alignment with organizational objectives and industry standards.
- Ensure compliance with legal and regulatory requirements for ICT operations.
- Serve as the final authority for approving exceptions to the policy.
- Ensure that the ICTMS team is adequately resourced and that staff are trained and competent to handle their roles.
- Monitor the effectiveness of ICT security and technology initiatives.
- Provide regular reports and updates to senior management on ICT performance and issues.

b. **Infrastructure Team:**

- Design, implement, and maintain the organization's IT infrastructure, ensuring high availability, scalability, and security.

- Ensure that all hardware and network devices are properly configured and meet organizational standards.
- Manage server environments, databases, network equipment, and cloud infrastructure.
- Oversee the installation, configuration, and management of all physical and virtual infrastructure systems.
- Monitor system performance and implement necessary upgrades or optimizations.
- Collaborate with the Cyber Security Team to ensure all infrastructure components meet security standards.

c. **Cyber Security Team:**

- Protect the organization's IT systems from cyber threats by implementing and maintaining appropriate security measures.
- Conduct regular security assessments and vulnerability testing of systems and applications.
- Monitor and respond to security incidents, ensuring rapid containment and mitigation of threats.
- Ensure all ICT systems are protected with up-to-date firewalls, antivirus software, and other security protocols.
- Develop and implement policies for secure data storage, access control, and user authentication.
- Provide training and awareness to employees regarding security best practices.

d. **Computer Maintenance Technologist:**

- Ensure the proper maintenance and repair of all hardware, including desktop computers, laptops, and peripheral devices.
- Perform routine hardware diagnostics and troubleshooting to resolve any issues promptly.
- Manage the lifecycle of IT hardware, including deployment, upgrades, and disposal in accordance with policy guidelines.
- Maintain an inventory of all hardware assets and ensure that they are registered, tracked, and updated as necessary.
- Provide technical support for hardware-related issues and assist users with installations, configurations, and troubleshooting.

e. **ICT Support Team:**

- Provide technical assistance and support for all ICT-related issues raised by employees.
- Resolve issues related to hardware, software, networking, and applications in a timely manner.
- Maintain and update knowledge base articles and user documentation to assist in troubleshooting common problems.

- Ensure that all support requests are logged, tracked, and resolved according to the service level agreements (SLAs).
- Facilitate remote support tools to address technical issues without the need for on-site intervention.
- Assist in the training and onboarding of new employees regarding the use of ICT resources and best practices.

f. **Administrative Assistance:**

- Support the ICTMS team with administrative tasks, including document management, meeting coordination, and communication with other departments.
- Assist with maintaining records of ICT policies, procedures, and user access documentation.
- Manage scheduling, correspondence, and logistics for ICT-related training sessions, audits, or team meetings.
- Maintain an inventory of all ICT-related documents and ensure they are up-to-date and accessible to authorized personnel.
- Coordinate the submission of IT-related support requests and escalate issues as needed.

g. **Software Quality Assurance Team:**

- Develop and enforce standards for software development and testing to ensure applications meet security, performance, and usability requirements.
- Conduct testing of internally developed applications to identify and resolve bugs, vulnerabilities, and performance issues.
- Perform both manual and automated testing to validate software functionality, security, and compatibility across different platforms.
- Work closely with programmers and other development teams to ensure that applications adhere to the established coding standards and quality benchmarks.
- Document and report testing outcomes, ensuring that all defects are tracked and addressed before software is released.

h. **Programmers:**

- Design, develop, and maintain software applications based on organizational requirements.
- Ensure that all code adheres to the organization's secure coding standards and best practices.
- Collaborate with the Software Quality Assurance Team to ensure applications undergo proper testing before deployment.
- Troubleshoot and fix bugs and issues that arise during development, testing, and after deployment.
- Implement new features and updates in existing applications, following change management protocols.

- Keep abreast of emerging technologies and incorporate relevant innovations into the organization's software solutions.

- **Enforcement**: Violations of this policy will result in appropriate disciplinary actions, including but not limited to warnings, suspension, or termination of access to IT systems and services.

  The following actions or violations are prohibited under the **Data Privacy Act of 2012** (Republic Act No. 10173) and may lead to disciplinary actions:

  1. **Unauthorized Collection of Personal Data:**
     - Collecting personal data without the consent of the data subject, or without lawful basis, is a violation of the Data Privacy Act.
     - Failure to inform individuals of the purpose for which their personal data is being collected.
  2. **Failure to Secure Personal Data:**
     - Not implementing adequate security measures to protect personal data against unauthorized access, disclosure, alteration, or destruction.
     - Failure to use encryption, firewalls, and other security controls to protect sensitive data.
     - Allowing unauthorized persons to access, process, or store personal data.
  3. **Sharing Personal Data Without Consent:**
     - Disclosing or sharing personal data with unauthorized persons or third parties without the consent of the data subject or a lawful basis.
     - Transferring personal data to other entities that do not comply with the Data Privacy Act's requirements for data protection.
  4. **Retention of Personal Data Beyond Retention Period:**
     - Retaining personal data longer than necessary for the fulfillment of its purpose or for compliance with legal obligations.
     - Failing to implement policies and procedures for data deletion or anonymization once the data is no longer required.
  5. **Failure to Comply with Data Subject Rights:**
     - Not providing individuals with the ability to access, correct, update, or request the deletion of their personal data as stipulated in the Data Privacy Act.
     - Not honoring a data subject's request for portability, blocking, or erasure of their personal data in cases where they have exercised their rights.
  6. **Failure to Report Data Breaches:**
     - Failure to notify the National Privacy Commission (NPC) and affected individuals within the prescribed time frame following a data breach.
     - Not taking immediate corrective actions or preventive measures following a data breach to protect personal data from further harm.
  7. **Unlawful Processing of Personal Data:**
     - Processing personal data without a lawful basis, such as obtaining consent, fulfilling contractual obligations, compliance with legal duties, protection of vital interests, public tasks, or legitimate interests.

- Using personal data for purposes beyond what was originally communicated to the data subject.

8. **Failure to Conduct Privacy Impact Assessments (PIA):**
   - Not conducting a Privacy Impact Assessment (PIA) for new projects or systems that involve the processing of personal data, especially when there is a risk of harm to the rights and freedoms of data subjects.
9. **Inadequate Training and Awareness on Data Privacy:**
   - Failing to provide employees with adequate training on data privacy policies, regulations, and their responsibilities in handling personal data.
   - Not ensuring that employees are aware of the proper handling, storage, and sharing of personal data in accordance with the Data Privacy Act.
10. **Failure to Appoint a Data Protection Officer (DPO):**
    - Not designating a Data Protection Officer (DPO) or not ensuring that the DPO has sufficient resources and authority to perform their role effectively, including overseeing compliance with data privacy requirements.

Consequences of Violations:

- **Warnings**: Employees may receive written warnings for minor infractions or first-time violations.
- **Suspension**: Suspension from accessing IT systems or services for repeated or severe violations, pending further investigation.
- **Termination of Access**: Immediate revocation of access to sensitive data or IT systems in cases of gross negligence or deliberate breaches of the Data Privacy Act.
- **Disciplinary Action**: Employees found guilty of violating the Data Privacy Act may face further disciplinary measures, including suspension, termination of employment, or legal action depending on the severity of the violation.

- **Review and Updates**: This policy will be reviewed annually and updated as necessary to ensure its continued effectiveness and alignment with security best practices and legal requirements.
- **Exceptions**: Any exceptions to this policy must be approved by ICTMS and documented with a risk assessment and mitigation plan.