ALDEN Q. QUIÑONES
IT Protection and Security: MIT 264

PASSWORD POLICY

POLICY:

This policy establishes requirements for creating and maintaining secure passwords to protect the company's information systems and ensure the confidentiality and integrity of sensitive data. This policy aims to reduce the risk of unauthorized access and data breaches caused by weak, stolen, or compromised passwords. In compliance with the Republic Act No. 10173 (Data Privacy Act of 2012), this policy is designed to safeguard the personal data of individuals and ensure that all data processing activities within the organization adhere to the highest standards of security and privacy. The policy seeks to mitigate risks associated with unauthorized access, data breaches, and the unlawful processing of personal data, in line with the Data Privacy Act's provisions on data protection, confidentiality, and the rights of data subjects.

OBJECTIVE:

The objective of this policy is to reduce the risk of unauthorized access to the company's critical systems, applications, and sensitive data by enforcing robust password standards. By establishing stringent password requirements, the policy seeks to safeguard the confidentiality, integrity, and availability of company data, uphold the security of digital infrastructures, and ensure compliance with industry-specific security regulations and best practices.

SCOPE:

This policy applies to all employees, contractors, third-party vendors, and authorized personnel who have access to the DSWD's information systems, applications, and devices, particularly those related to the Pantawid Pamilyang Pilipino Program (4Ps). This includes, but is not limited to, systems used for the registration, monitoring, and disbursement of financial aid to beneficiary families, as well as any associated data platforms.

The policy covers access to all DSWD and 4Ps-related digital systems, including but not limited to:

- Workstations and desktops used to access or manage 4Ps information.
- Mobile devices used by field officers, including smartphones and tablets for on-the-ground data collection and verification.
- Cloud-based platforms used for data storage, analytics, and communication within the scope of the Pantawid Pamilyang Pilipino Program.
- Databases that store sensitive beneficiary data, case records, and program-related documentation.
- Applications that manage the program's beneficiary registry, financial assistance distribution, and reporting systems.
- Any other systems where passwords are required to authenticate user access to 4Ps information and data.

REFERENCE:

1. Republic Act No. 10173 (Data Privacy Act of 2012): This law establishes the legal framework for the protection of personal data in the Philippines, ensuring the confidentiality, integrity, and security of sensitive personal information collected by both public and private entities.
2. Republic Act No. 10175 (Cybercrime Prevention Act of 2012): This act defines and penalizes cybercrimes, including illegal access, interception, and misuse of data and information systems. It aims to protect information systems from unauthorized access and cyberattacks.
3. National Privacy Commission (NPC) Circulars and Issuances: These include guidelines issued by the NPC that ensure compliance with the Data Privacy Act and set standards for the security and management of personal data, including encryption, access control, and data breach notifications.

4. Republic Act No. 8792 (E-Commerce Act of 2000): This law covers the use of electronic transactions and establishes guidelines for ensuring the security of electronic data, particularly in relation to digital signatures and other electronic authentication methods.
5. Department of Information and Communications Technology (DICT) Cybersecurity Manual: A comprehensive guide for government agencies to enhance cybersecurity measures, including the protection of sensitive data and information systems from unauthorized access or breaches.
6. Philippine National Standard (PNS) ISO/IEC 27001: This standard outlines the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system (ISMS) tailored to the Philippine context.
7. Cybersecurity Act of 2015 (Republic Act No. 10844): This act creates the Department of Information and Communications Technology (DICT) and mandates it to implement policies and programs related to cybersecurity, including the protection of government information systems.

DEFINITIONS:

- **Password**: A secret string of characters used for authentication and gaining access to systems or information.
-
- **Password Expiry**: The process by which passwords are set to expire after a defined period and require the user to create a new one.

GUIDELINES:

1. **Minimum Length**: Passwords must be at least **8 characters** in length.
2. **Required Character Types**: Passwords must include at least three of the following:
    - Uppercase letters (A-Z)
    - Lowercase letters (a-z)
    - Numbers (0-9)
    - Special characters
    - Password must not same with the username
3. **Password Expiry Period**: Passwords must be changed every **90 days**. Users will be prompted to update their passwords 30 days before expiration.
4. **Password History**: Users cannot reuse any of the last **5 passwords**.
5. **Password Storage**: Password must be stored in a secured platform like google/azore password manager
6. **Password Complexity**: Simple, common passwords are prohibited. Passwords must not contain easily guessable information like names, birthdates, or company details.
7. **Multi-factor Authentication (MFA)**: MFA must be enabled for all critical systems and applications, such as email, VPN, cloud storage, and internal platforms.

ADMINISTRATION:

- **Responsibilities**:

    - **Regional ICT Officer (RICTO)**: Responsible on overseeing all IT operation from Password Policy Implementation, ICT Support, System Development, and Infrastructure.
    - **ICT Support Team:** Responsible in addressing ICT Related Issues and concerns.
    - Responsible for implementing, monitoring, and enforcing the password policy.
    - **Infrastructure Team:** Responsible in conducting periodic ICT infrastructure maintenance routine like preventive, protective, corrective maintenance.
    - **Cyber Security Team:** Responsible in systems audit and addressing cyber security issues.
    - **Software Quality Assurance (SQA) Team:** Responsible in system analysis and database designs.

    - **Employees**: Responsible for adhering to the password guidelines and maintaining the confidentiality of their passwords.

- **Policy Enforcement**:

  Violations of this policy may result in disciplinary action, including account suspension, mandatory retraining, or further consequences depending on the severity of the violation.

- **Review & Updates**:

  This policy will be reviewed annually by the IT Security team and updated as necessary to ensure compliance with industry standards and regulations.