500 Password Policy v2

500 PASSWORD POLICY

500.1 Introduction:

The purpose of this Password Policy is to establish guidelines for creating strong, secure, and confidential passwords to protect the Archdiocese of Baltimore's systems, data, and network resources from unauthorized access and potential security breaches.

500.2 Purpose:

This policy applies to all employees, volunteers. contractors. and any individuals who have access to the Archdiocese of Baltimore's systems, data, and network resources.

500.3 Password Creation Guidelines:

3. 1. Complexity Requirements

a. Password Length: Passwords must be a minimum of 8 characters in length.

b. Complexity: Passwords must include a combination of upper and lowercase letters, numbers, and special characters.

c. Avoid Common Patterns: Passwords should not contain common patterns, such as" 12345678″ or "password."

d. Avoid Personal Information: Passwords should not include personal information such as names, birthdays, or addresses.

3.2. Password Management

a. Unique Passwords: Each user must have a unique password for their individual accounts. Password reuse across multiple systems or accounts is strictly prohibited.

b. Regular Password Changes: Users must change their passwords at least

every 90 days. Passwords should not be reused within a 12-month period.

c. Restricted Sharing: Passwords must not be shared with others or stored in an insecure manner, such as writing them down or storing them in plain text files.

d. Password Reset: If a password is forgotten or compromised, users must follow the organization's password reset procedures to regain access to their accounts.

500.4 Password Protection:

4.1. Password Storage: Passwords should be stored securely using industry-standard encryption methods. Plaintext storage of passwords is strictly prohibited.

4.2. Account Lockouts: After a certain number of failed login attempts, user accounts will be temporarily locked to prevent unauthorized access. Users must follow the organization's account unlocking procedures to regain access.

4.3. Two-Factor Authentication (2FA): Two-Factor Authentication is strongly recommended for all accounts where technically feasible. It adds an extra layer of security by requiring users to provide additional authentication factors along with their passwords.

500.5 Employee Responsibilities:

5.1. Password Confidentiality: Users must keep their passwords confidential and not share them with anyone, including TT staff or supervisors.

5.2. Reporting Suspicious Activity: Users must promptly report any suspected unauthorized access or suspicious activity related to their passwords or accounts to the IT department or designated IT security contact.

500.6 Compliance and Enforcement:

6.1 . Compliance Monitoring: The Archdiocese of Baltimore reserves the right to monitor password usage and enforce compliance with this policy.

6.2. Consequences of Non-Compliance: Failure to comply with this Password Policy may result in disciplinary actions, including account suspension. loss of access privileges, and potential legal consequences.

500.7 Policy Review:

This Password Policy will be reviewed on a periodic basis to ensure its effectiveness and compliance with evolving security standards and best practices.

Please note that this is a general example and should be customized to fit the specific needs and requirements of the Catholic organization. It is recommended to seek legal advice and consult with relevant stakeholders when drafting or implementing a Password Policy.