Enhanced Password Policy for [Healthcare Organization Name]

Introduction

The purpose of this Enhanced Password Policy is to establish stringent guidelines for creating, managing, and maintaining secure passwords within [Healthcare Organization Name], which encompasses three hospitals and 25 clinics. This policy is designed to protect the organization's information systems and sensitive data, especially patient health information, from unauthorized access and potential breaches.

Scope

This policy applies to all individuals (employees, contractors, and affiliates) who have been granted access to any system, application, or device requiring password authentication within the [Healthcare Organization Name] network.

Policy Details

1. **Password Complexity and Construction**
   - **Minimum Length**: Passwords must be at least 16 characters in length to enhance security against brute-force attacks.
   - **Composition**: Passwords must include a mix of the following character types:
     - Uppercase letters (A-Z)
     - Lowercase letters (a-z)
     - Numbers (0-9)
     - Special characters (e.g., @, #, $, %, &, *)
   - **Prohibited Terms**: Passwords must not contain common terms, such as names of seasons, sports teams, or easily guessable sequences (e.g., "password", "12345678"). They should also avoid personal information easily linked to the user, such as birthdates, anniversaries, or names of family members and pets.
2. **Password History and Reuse**
   - Users are prohibited from reusing their last 8 passwords to prevent the recycling of potentially compromised credentials and encourage the creation of unique passwords at each change interval.
3. **Exposed Password Check**
   - All new or changed passwords will be checked against databases of known exposed passwords (e.g., those revealed in data breaches). If a password is found in such a database, it will be rejected, and the user will be prompted to choose another password that is not compromised.
4. **Password Updates and Expiration**
   - Passwords must be changed at least every 90 days or sooner if suspected of being compromised.
   - Users will receive notifications starting 14 days before their password's expiration date, reminding them to change their password.
5. **Secure Password Storage and Handling**

    - Passwords must never be stored in plain text or in an insecure manner. Users are encouraged to use approved, encrypted password managers for storing complex passwords securely.
    - Sharing of passwords is strictly forbidden. Each user is responsible for the security of their passwords and any actions taken with their credentials.
6. **Automated Security Measures**
    - Systems will enforce the password complexity and history requirements automatically during password creation or change.
    - An account lockout policy will be implemented, locking user accounts for 15 minutes after five unsuccessful login attempts to mitigate brute-force attack risks.
7. **User Education and Training**
    - Regular training sessions and communications will be provided to all users, emphasizing the importance of strong, secure passwords and the overall role of password security in protecting sensitive information and systems.

Enforcement and Compliance

Failure to comply with this Enhanced Password Policy may result in disciplinary action, up to and including termination of employment. The IT department and security teams are responsible for enforcing this policy, conducting periodic audits, and ensuring system configurations adhere to these guidelines.

Policy Review and Modification

This policy will be reviewed annually and updated as necessary to adapt to new cybersecurity threats, technological advancements, and organizational changes.

By following this Enhanced Password Policy, all users contribute to the security and integrity of [Healthcare Organization Name]'s information systems and the protection of sensitive healthcare data.