Password Policy for [Healthcare Organization Name]

Introduction

This Password Policy establishes the standards for the creation, management, and use of passwords within [Healthcare Organization Name], encompassing three hospitals and 25 clinics. The policy aims to protect the confidentiality, integrity, and availability of our information systems and data, particularly sensitive patient information. This policy applies to all employees, contractors, and affiliates who have access to our systems and data.

Scope

This policy applies to all systems, applications, and devices that require password authentication to access information resources managed or owned by [Healthcare Organization Name].

Policy Details

1. **Password Complexity Requirements**
    - Passwords must be a minimum of 12 characters in length.
    - Passwords must contain at least one character from the following categories:
        - Uppercase letters (A-Z)
        - Lowercase letters (a-z)
        - Numbers (0-9)
        - Special characters (e.g., !, @, #, $, %)
2. **Password Change and Lifetime**
    - Passwords must be changed at least every 90 days.
    - Users must not reuse their last four passwords.
    - Temporary passwords provided for initial access or password resets must be changed upon the first login.
3. **Secure Password Storage and Transmission**
    - Passwords must not be stored in a readable format. Secure password managers are recommended for managing complex passwords.
    - Passwords must not be transmitted over unsecured channels. If password transmission is necessary, it must be encrypted using approved encryption methods.
4. **Password Protection**
    - Users are responsible for keeping their passwords confidential and must not share passwords with anyone, including colleagues, supervisors, or family members.
    - Passwords must not be written down or stored in an unsecured manner.
    - If a password is suspected to have been compromised, it must be changed immediately, and the incident reported to the IT department.
5. **Automated Password Controls**
    - Systems must enforce password complexity requirements and rotation policies automatically.
    - Account lockout mechanisms shall be employed on all systems to mitigate the risk of brute force attacks. After five unsuccessful login attempts, the account

should be locked for a minimum of 15 minutes or until unlocked by an administrator.

6. **User Education and Awareness**
    - [Healthcare Organization Name] will provide ongoing education and awareness training on the importance of strong passwords and the role they play in securing sensitive information.
    - Users will be informed about this policy and its requirements upon onboarding and through regular security awareness updates.

Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment. The IT department is responsible for monitoring compliance with this policy and conducting periodic audits to ensure its effectiveness.

Acknowledgment

All users are required to acknowledge receipt and understanding of this Password Policy as a condition of accessing [Healthcare Organization Name]'s information systems.

Review and Update

This policy will be reviewed annually and updated as needed to respond to new security threats, technological changes, and organizational needs.

By adhering to these password management guidelines, users contribute to safeguarding [Healthcare Organization Name]'s digital assets and protecting the privacy of our patients and staff.