Data Security Policy - Security Awareness and Training

PURPOSE

To provide rules for security awareness and training for members of the workforce, including management.

SCOPE

The Security Awareness and Training Policy and Procedure will cover:

- Security updates and reminders
- Security training for employees;
- Security awareness and training process, including
- Malware Training
- Social Engineering Training
- Password creation, modification, and protection
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- And Relevant Regulations, Standards, and Criteria.

POLICY

Fostering security awareness and providing training for Organization’s employees is key to protecting Organization from security threats and accidental errors. Organization wants to foster a security-aware culture.

Organization has adopted and followed a security awareness and training program for all members of the workforce (including management). Organization will require employees to complete security training in The Guard. Trainees will need to acknowledge that they completed and understood the training, and Organization will document all attestations.

Security Updates

To foster a security-aware culture, Organization will provide periodic security updates to the workforce, covering topics including:

- Security threats to ePHI that recently occurred or may occur
- Changes to Organization’s security program, policies, technologies, or procedures
- The importance of security to HIPAA and other regulatory and compliance efforts
- And other security updates relevant to the workforce

Organization may opt to use email newsletters, videos, webinars, and other forms of media or communications to provide security updates to the workforce.

Security Training

As part of Organization’s security awareness and training program, we will provide security training to employees upon hire and annually. Employees, including management, are required to complete security training and acknowledge that they have completed training. Training logs need to be retained for compliance purposes.

Social Engineering Training

Social engineering attempts, including phishing, involve using a fake communication, like an email, phone call, or text message, to trick users into providing a bad actor with confidential data or passwords. This is a common attack vector used by cybercriminals to breach organizations today, and Organization provides employees with training to identify and respond to potential social engineering attempts.

Password Management Training

Creating and protecting passwords and secrets can make all the difference in security.

Organization’s security training will provide employees with instructions on creating and protecting strong passwords.

PROCEDURES

Organization will review and update this Security Awareness and Training Policy and Procedure at least annually.

If Organization determines that additional training is required for a subset of workforce members, such as system owners and administrators, the company will make those resources available.

Workforce members who fail to demonstrate a clear understanding of security awareness may be required to complete additional or supplemental training.

Security Updates

Organization sends security updates to employees at least quarterly via company email. The company will post signs and reminders in physical workspaces to remind employees about security best practices.

Security Training

Organization's Security Training includes:

- Information on Organization's security policies, procedures, and technologies
- Procedures for protecting company devices from malicious software, including:
    - Potential harm that can be caused by malware
    - Malware prevention, and how malware prevention software works
    - What to do in the event of a malware infection
    - How to report a potential malware infection
- Procedures for handling social engineering attempts
    - Ways to identify suspicious emails, texts, and communications
    - What to do if targeted by a phishing or social engineering attack
    - How to report a potential attack attempt
- Procedures for creating strong passwords and safeguarding secrets
- Policy and Procedure for Incident Response and Reporting
- Policy and Procedure for Workstation Use and Workstation Security
- Changes to Organization's security program
- Other security topics relevant to Organization

You may use The Guard's Training and Policy Modules and materials to achieve these control objectives.

Freshness of Security Awareness Training

Organization will ensure that all new members of the workforce receive security awareness training on hire and on at least an annual basis.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(5)(i) *Security awareness and training*
- §164.308(a)(5)(ii)(A) *Security reminders*
- §164.308(a)(5)(ii)(B) *Protection from malicious software*
- §164.308(a)(5)(ii)(C) *Log-in monitoring*
- §164.308(a)(5)(ii)(D) *Password management*

RELEVANT SOC 2 CRITERIA:

- CC 1.4.3: *Attracts, develops, and retains individuals.*
- CC 1.4.7: *Provides training to maintain technical competencies.*
- CC 2.2.6: *Communicates information on reporting failures, incidents, concerns, and other matters.*
- CC 2.2.8: *Communicates information to improve security knowledge and awareness.*
- CC 2.3.6: *Communicates objectives related to confidentiality and changes to objectives.*
- CC 2.3.11: *Communicates information on reporting system failures, incidents concerns, and other matters.*
- CC 6.7.1: *Restricts the ability to perform transmission.*
- CC 6.7.2: *Uses encryption technologies or secure communication channels to protect data.*
- CC 6.7.3: *Protects removal media.*
- CC 6.7.4: *Protects mobile devices.*

APPENDIX A: PASSWORD SECURITY BEST PRACTICES

NIST recommends the following password standards for creating strong passwords:

- Use a minimum of eight (8) characters, with longer passwords being more secure
- Disallow or do not use sequences or repetitive characters, such as “12345” or “aaaaa”
- Disallow or do not use context-specific passwords, like the name of the site or company
- Disallow or do not use commonly used passwords, such as “password123” and “12345678”
- Disallow or do not use single dictionary words
- Disallow or do not use passwords that have been compromised previously

In addition, the company encourages the following password best practices:

- Do not share passwords with others
- If you suspect that your password has been compromised, change your password immediately and report the incident
- Do not reveal passwords over the phone or via email
- Do not provide password hints
- Do not use another user’s username and password
- Do not write down usernames and passwords