**Security Awareness Program Training Policy**

**Overview:**

[Insert Covered Entity or Business Associate name] is responsible for ensuring the confidentiality, integrity, and availability of all Protected Health Information (PHI) stored on its systems. [Insert Covered Entity or Business Associate name] has an obligation to provide appropriate protection against threats, which could adversely affect the security of the system or its data entrusted on the system. Implementation of this policy will limit the exposure and possible effects of common threats to the systems.

**Scope:**

The security awareness program is designed to educate all users on the security policy for [Insert Covered Entity or Business Associate name].

**Definitions:**

1. Email: The electronic transmission of information through a mail protocol such as SMTP, POP, or IMAP.
2. User: any employee or other person authorized by [Insert Covered Entity or Business Associate name] to read, enter or update information created or transmitted via the electronic mail system.

**Policy:**

1. The Security Officer will be responsible for implementing and ensuring this policy is followed by all employees.
2. The Security Officer may/will create a Security Awareness Training Team to help implement the training.
3. The security awareness training for workforce members should focus on:
	1. Employee responsibility for computer security
	2. Impact of unauthorized access
	3. Address the quickly and ever-changing data security threat environment
	4. Educating users on the creation of good passwords
	5. How to properly maintaining workstations
	6. Avoiding malicious software
	7. Informing users of email and Internet access policies, including:
		1. Tools used to monitor usage
		2. How to identify social engineering tactics
		3. Social media usage
	8. Physical security
	9. Reporting procedures
	10. Emergency procedures
4. The security awareness training for system administrators should include:
	1. Training on how to configure systems securely
	2. Education on user account management policies
	3. Secure remote access for support of systems
5. New employees will be required to take this training within the first month of employment.
6. Training will be conducted annually, during a time specified by the Security Officer/ Security Awareness Training Team. [Insert Specified timeframe (eg. First week of March)]
7. The Security Officer/ Security Awareness Training Team may/will implement weekly/monthly security training updates.
	1. All users are required to read these updates and implement any changes.

**Violations:**

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment. Violations shall be noted in the [Insert Covered Entity or Business Associate name] issue tracking system and support teams shall be dispatched to remediate the issue.