**Insert Here Logo**

**Security Awareness and Training Policy**

**CONFIDENTIAL INFORMATION**

This document is the property of ABC Organization: it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the document owner. Dissemination, distribution, copying, or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of ABC Organization **Copyright © 2022**

**Table of Contents**

[Document Revision History 2](#_Toc123725303)

[1 Security Awareness and Training Policy 3](#_Toc123725304)

[1.1 Purpose 3](#_Toc123725305)

[2 Policy 4](#_Toc123725306)

[2.1 Security Reminders 4](#_Toc123725307)

[2.2 Protection from Malicious Software 4](#_Toc123725308)

[2.3 Log-in Monitoring 4](#_Toc123725309)

[1. Password Management 4](#_Toc123725310)

[1. Security Training Program 5](#_Toc123725311)

[2.4 Violations 5](#_Toc123725312)

# Document Revision History

|  |  |
| --- | --- |
| **Author(s)** |   |
| **Status** | Version 1.0 |
| **Distribution** |  |
| **Reviewers** | **Date** | **Version** | **Description** | **Comments** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Security Awareness and Training Policy

## Purpose

 ABC Organization is committed to protecting Personal Health Information in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). ABC Organization has adopted this policy to provide security awareness and training for all members of its Workforce. This Policy covers security reminders, procedures for guarding against, detecting and reporting malicious software, procedures for monitoring log-in attempts and reporting discrepancies and procedures for creating, changing and safeguarding passwords.

# Policy

## Security Reminders

* ABC Organization has established procedures on how the ABC Organization departments and users will be notified of periodic updates of security changes in HIPAA security policies and procedures and ABC Organization’s general security policies.
* ABC Organization has established procedures on how to notify departments and users of any warnings that are issued for discovered, reported or potential threats.

## Protection from Malicious Software

* ABC Organization will provide training to all its users on how to identify and protect against malicious code and software.
* Information Systems will develop and implement procedures to detect and guard against malicious code such as viruses, worms, ad ware, and any other computer program or code designed to interfere with normal operation of a system.
* A virus detection system must be implemented on all workstations including a procedure to ensure that the virus detection software is maintained and up to date.
* Information Systems will notify all departments and users of new and potential threats from malicious code such as viruses, worms, denial of service attacks, and any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.
* Departments and users must notify Information Systems if a virus, worm or other malicious code has been identified.
* Information Systems will be responsible for ensuring that any system that has been infected by a virus, worm or other malicious code is immediately cleaned and properly secured or isolated from the rest of the network.
* See the ABC Organization Technology Policy section titled “Security Policy Methodologies” for details.

## Log-in Monitoring

* Information Systems will implement a mechanism to log and document failed login attempts on each system containing Medium and high-risk PHI.
* Information Systems will review such log-in activity reports and logs on a periodic basis.
* Procedures for reviewing logs and activity reports will be created by Information Systems and detailed in the Audit control review plan.
* All failed log-in attempts of a suspicious nature, such as continuous attempts, must be reported to the HIPAA Security Officer.

## Password Management

* Information Systems will develop and implement procedures for creating, changing, and safeguarding passwords.
* These minimum procedures will be followed:
	+ All users including ABC Organization employees, vendors, and agencies who use a computer or has access to network resources or systems will have a unique user identification and password.
	+ All computers, network resources, system and applications will require the user supply a password in conjunction with their unique user identification to gain access.
	+ A role-based user identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to PHI. Access to PHI will be permitted if there is a second unique user id and password required.
	+ All passwords will be of sufficient complexity to ensure that it is not easily guessable by dictionary attacks.
	+ Elected Official and Department Heads will be responsible for making their employees aware of all password-related policies and procedures, and any changes to those policies and procedures.
	+ Information Systems will be responsible for setting password aging times for systems, networks and applications.
	+ All ABC Organization employees are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:
		- Passwords are only to be used for legitimate access to networks, systems, or applications.
		- Passwords must not be disclosed to other users or individuals.
		- Employees must not allow other employees or individuals to use their password.
		- Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

## Security Training Program

ABC Organization will ensuring that its Employees have been given the appropriate level of HIPAA security training so that all Employees who access, receive, transmit or otherwise use PHI are familiar with Security policies and procedures and their responsibilities regarding such policies and procedures. Training will consist of the following:

* HIPAA Security Policies
* HIPAA Business Associate Policy
* HIPAA Sanction Policy
* Confidentiality, integrity and availability
* Individual security responsibilities
* Common security threats and vulnerabilities

In addition those who set up, manage or maintain systems and workstations will receive this training;

* Password structure and management procedures
* Server, desktop computer, and mobile computer system security procedures, including security patch and update procedures and virus and malicious code procedures
* Device and media control procedures
* Incident response and reporting procedures

## Violations

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.