|  |
| --- |
| **TITLE: Security Awareness Training Policy**  |
| **DEPARTMENT: Information Technology and Human Resources** |
| **Effective Date:** | **Revised Date:** | **Next Review Date:** |
|  |  |  |
| **Prepared by: Donny Friday, Director of IT** | **Date: 05/31/21** |
| **Administrative Approval:** Chief Executive Officer, Chief Information Officer, and Compliance Officer |
| CEO: Joe LaRue | Date:  |
| CIO: Chip Burns | Date:  |
| CO: Sharon Grambow | Date:  |
| **All other related polices/procedures/protocols:**  |

SEE LAST PAGE FOR REVIEW HISTORY

**Purpose:**

The purpose of this policy is to ensure that all Sun Health employees and affiliates who have been granted access to organizational data, are taught Information Security Awareness in order to gain an understanding of the importance of securing the organizations data. Sun Health seeks to establish a culture that ensures that institutional data is secure. This policy and associated procedures establish the minimum requirements for the Security Awareness and Training controls.

**Scope and Applicability**

This policy applies to all Workforce Members, including management, vendors, and business associates, that utilize or have access to Information Systems.

**Policy Statement**

Sun Health employees are required to complete formal security awareness training when granted access to any Information Systems and at least annually thereafter. Training will be coordinated with Human Resources. All users shall be given appropriate end user training for the Information Systems to which they are granted access to.

**Procedures**

**General**

1. A security awareness and training program shall be implemented for all members of its workforce including management.
2. HR and IT shall review all training programs, and revise if needed, on an annual basis.

**User Training**

1. General computer security awareness and end user training programs are available to all Sun Health users including but not limited to:
	1. Acceptable use of Information Systems;
	2. Confidentiality and handling requirements of ePHI and other Sensitive information;
	3. Guarding against and reporting malicious software;
	4. Creating, changing, and safeguarding strong passwords;
	5. Monitoring of log-in attempts and discrepancies;
	6. Physical security of Information Systems including protecting output from displays and printers;
	7. Reporting of potential or suspected security incidents.
2. Sun Health work force members shall participate in training programs as part of initial training for new Users and when required by system changes.
3. Sun Health work for members shall receive training prior to being granted access to Information Systems. In the event that an exception must be granted for individual Users, training must be conducted within 30 days of receiving access.
4. Sun Health work force members shall receive refresher security awareness training on an annual basis.

**System and Security Personnel Training**

1. Workforce members with security and compliance related roles shall receive specialized HIPAA Privacy and Security related training on an annual basis, including:
2. Application managers, system and network administrators, super users;
3. Personnel who have access to system-level software and/or elevated privileges;
4. Physical security personnel;
5. Compliance and Risk management personnel.

**Security Reminders and Advisories**

1. Security awareness reminders shall be provided by IT to Sun Health work force members on a periodic basis.
2. Incident or event driven security advisories shall be distributed by IT to Sun Health work for members as appropriate.

**Security Training Records**

1. Security awareness training records shall be developed and retained for individual Users.

**Enforcement & Exception Handling**

Failure to comply with this policy, associated procedures and guidelines may result in disciplinary actions up to and including termination of employment or termination of contracts. Legal actions also may be taken for violations of applicable regulations and laws.

Request for exceptions to this policy must be submitted in writing. Prior to official approval of any exception, this policy must continue to be observed.

**Definitions**

**ePHI** - Protected Health Information that is stored in electronic format.

**Information System** –Meansany combination of [information technology](http://en.wikipedia.org/wiki/Information_technology) and people's activities that support operational, management and decision-making processes. A system normally includes hardware, software, information, data, applications, communications, and people.

**Users** -Are the individuals, groups, or organizations authorized to access information assets.

**Workforce Member** -Means employees and other persons whose conduct, in the performance of work, are under the direct control of the organization, whether or not they are paid by the organization. This includes full and part time employees, contractors, affiliates, associates, students, and volunteers.

**Distribution**

This policy should be distributed to applicable Workforce Members. Recipients of this policy must acknowledge their receipt and understanding of this policy by referring any questions or problems with the policy within ten days of the issue date to the HIPAA Security Officer. If no questions or problems are stated, it will be assumed that the policy has been read and understood.

**Applicable Regulations**

|  |  |
| --- | --- |
| **HIPAA Security Rule** | **45 CFR Part 160 and Subparts A and C of Part 164** |
| Security Awareness and Training  | §164.308(a)(5)(i),  |
| Security Reminders | §164.308(a)(5)(ii)(A) |
| Protection from Malicious Software | §164.308(a)(5)(ii)(B) |
| Log-in Monitoring | §164.308(a)(5)(ii)(C) |
| Password Management | §164.308(a)(5)(ii)(D) |

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date: | Reviewed/Revised by: | New Changes | No Change | Revision(s): State reason for revision | INITIALS |
| √ one |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |