|  |
| --- |
| **POLICY: Third Party Vendor Access** |
| *Original Implementation Date:* |  | *Date Reviewed/ Revised:* | April 16, 2018 | *Area of Responsibility:* | Technology | *Version:* | *1.0* |

**PURPOSE:**To establish policy governing security requirements for all Third Party Vendors and Business Associates. The following documents are used in conjunction with this policy:

Business Associate Agreement

Vendor Certification Form

Third Party Access Agreement

This policy applies to any and all Sun Health Senior Living owned equipment, personal equipment used on Sun Health Senior Living networks or vendor equipment used on Sun Health Senior Living networks.

**DEFINITIONS**

Audit – Means an inspection and verification of records.

Compliant – Means conforming to the accepted standard.

Standards – Means a set of requirements to maintain a secure environment.

**POLICY:**All Sun Health Senior Living third-party vendors and business associates are required to implement, test and continually monitor the administrative, physical, and technical controls outlined below to protect Sun Health Senior Living sensitive data (including, but not limited to, protected health information, financial data, credit card information, and employee data).

The security controls described below are required in addition to any requirements as set forth by Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI DSS) or other applicable regulations.

**PROCEDURES:**

Authentication and Access Control

1. All vendors and business associates must have a formal, documented process for granting and revoking access to all systems that process or store Sun Health Senior Living sensitive data.
	1. Vendor and business associate user access rights shall be strictly limited to a need-to-know basis that permits access only to the systems and resources that are required for users to perform their duties
	2. All vendors and business associates users with authorized access to Sun Health Senior Living sensitive data must be assigned a unique User ID which must not be shared with any other individual
2. For single-factor authentication solutions, passwords managed by vendors and business associates or implemented within vendors and business associates provided applications that are used to authenticate to systems processing or storing Sun Health Senior Living sensitive data must meet or exceed the following minimum requirements:
	1. All passwords shall have at least eight (8) characters. Applications not integrated with Sun Health Senior Living Active Directory must technically enforce this requirement
	2. Passwords shall contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and punctuation
	3. Passwords shall not be constructed of a single word found in the dictionary. Passphrases constructed of multiple words are acceptable as long as they meet the other criteria outlined in this section
	4. Users shall not be permitted to construct passwords that are identical or substantially similar to passwords that they had previously employed
	5. Passwords and any application or system passwords protecting Sun Health Senior Living sensitive data shall be changed at least every 12 months
	6. Passwords must be hashed (with unique salts) and stored securely. In addition, any public-facing systems must use a slow hashing algorithm that implements a work factor (such as PBKDF2, bcrypt, or scrypt). Clear text storage or reliance only on reversible encryption algorithms to protect passwords is not authorized. Authenticators used in multi-factor authentication mechanisms (such as PKI or biometrics) must be afforded the same secure storage protections
3. Access rights will be revoked immediately upon termination of any vendor and business associate user with access to Sun Health Senior Living systems or resources or in the event that a change in job role eliminates the requirement for continued access.
4. All access rights must be reviewed by vendor and business associate no less frequently than once annually.
5. All vendor and business associate user access to systems storing Sun Health Senior Living sensitive data must be audited and those audit records be maintained and made available to Sun Health Senior Living upon request.

Data Transmission, Confidentiality and Integrity

1. All Sun Health Senior Living sensitive data transmitted by vendors and business associates will be protected with a transmission encryption solution that complies, as appropriate, with NIST Special Publications 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others, which are Federal Information Processing Standards (FIPS) 140-2, validated.
	1. Approved solutions are limited to those that have been issued a FIPS 140-2 Validation Certificate
	2. Data transmissions include, but are not limited to web transmissions, file transfers, and email

Media Protection, Sanitization and Destruction

1. All Sun Health Senior Living sensitive data stored by vendors and business associates will be protected with a data-at-rest encryption product utilizing a Validated FIPS 140-2 Cryptographic Module with a 128-bit key or higher.
	1. Removable media and mobile devices will not be used by vendors and business associates users to store or transport any Sun Health Senior Living sensitive data unless explicitly approved, in writing, by the Sun Health Senior Living Infrastructure Administrator. Such approved solutions will be limited to those that have been issued a FIPS 140-2 Validation Certificate
	2. Applicable data storage includes (but is not limited to) storage of sensitive data on servers, workstations, and backup media (disk or tape) as well as any approved storage of Sensitive Data on removable media or mobile devices (to include phones, tablets, CD/DVD, USB thumb drives)
2. Upon termination of the contract with Sun Health Senior Living or at any time prior to reuse or repurposing of media used to store or process Sun Health Senior Living sensitive data, said media must be cleared (using a DoD-compliant 7-pass wipe) or purged in accordance with NIST SP 800-88.
	1. If the media is to be destroyed, the method used must ensure that after destruction, the media is able to withstand a laboratory attack as outlined in NIST SP 800-88
	2. vendors and business associates must provide a certificate of destruction if requested by Sun Health Senior Living

System Security and Vulnerability Management

1. Vendors and business associates must have a documented patch management and distribution process that ensures security patches are applied to all systems (to include servers, workstations, laptops) that process and/or store Sun Health Senior Living sensitive data.
	1. All critical security patches must be deployed within 30 days of vendor release unless otherwise discussed and approved, in writing, by the Sun Health Senior Living Infrastructure Administrator.
2. Vendors and business associates must employ network security architectural components (to include, at a minimum, firewalls and network intrusion detection/prevention solutions) to adequately protect all systems processing or storing Sun Health Senior Living sensitive data that are accessible from the Internet or other public network.
3. Vendors and business associates must employ an anti-virus solution with real-time protection and automatic updates on all systems that store or process Sun Health Senior Living sensitive data.
4. Vendors and business associates will ensure any web-based solutions storing or processing Sun Health Senior Living sensitive data will adhere to security design best practices including, but not limited to, protecting against the Open Web Application Security Project OWASP Top 10 list of security risks.

Auditing

1. All systems that process or store Sun Health Senior Living sensitive data must maintain an automated audit trail that documents system security events as well as any event that results in the access, modification, and/or deletion of Sun Health Senior Living sensitive data.
2. The audit trail must, at a minimum record the following information for each event:
	1. Type of event occurred
	2. When (date and time) the event occurred
	3. The source of the event
	4. The outcome (success or failure) of the event
	5. The identity of any user/subject associated with the event
3. Audit logs must be read-only and protected from unauthorized access. Audit records documenting events resulting in the access, modification, and/or deletion of Sun Health Senior Living sensitive data must be made available to Sun Health Senior Living upon request.
4. Vendors and business associates must employ a regular audit log review process (either manually or automated) for detection of unauthorized access to Sun Health Senior Living sensitive data.

Remote Access

1. Vendors and business associates must sign a Third Party Remote Access Agreement before being granted remote access to any Sun Health Senior Living information systems or resources
2. Unless otherwise explicitly approved and documented by the Sun Health Senior Living Infrastructure Administrator, all remote access must occur using the Sun Health Senior Living VPN solution, Citrix, LogMeIn, or WebEx as outlined in the Remote Access Agreement.

Physical Security

1. In addition to the previously mentioned technical controls, vendors and business associates must employ physical safeguards and visitor access controls to prevent unauthorized access to all systems and media used to process or store Sun Health Senior Living sensitive data.

Awareness and Training

1. Vendors and business associates must ensure all users receive regular security awareness training and are apprised of the requirements outlined within this agreement.

 Administration

1. All vendors and business associates that process or store Sun Health Senior Living sensitive data will sign a Business Associate Agreement (BAA).
	1. New BAAs are required with a change of signatory or contract renewal
2. All vendors and business associates that process or store Sun Health Senior Living sensitive data will complete a Vendor Certification form.
	1. New Vendor Certification forms are required with a change of signatory or contract renewal
	2. When a SSAE 16 report is unavailable or not applicable, vendors and business associates will submit the most recent risk assessment results
3. All non-compliant vendors and business associates will be referred to Sun Health Senior Living General Counsel.

Review and Revision

1. Third Party Vendor policy must be reviewed at least annually or sooner if warranted.

**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.

The Director of Information Technology will be responsible for performing tests of the internal controls of this policy for adequacy and completeness.

**POLICY SIGNATURE PAGE**

Approved by:

**\_\_\_Donny Friday\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_05/31/22\_\_\_\_\_\_\_\_\_\_**

Director of Information Technology Date

**RELATED POLICIES AND REFERENCES**

(Include manual name, section or chapter and other pertinent details; website name and link to the information of the website; any other information to locate details for reference.)

Example:
National Institutes of Health, Department of Health and Human Resources. www.nia.nih.gov/health. Accessed January 2018.