|  |  |  |
| --- | --- | --- |
| **TITLE: Information Classification Policy** | | |
| **DEPARTMENT: Information Technology** | | |
| **Effective Date:** | **Revised Date:** | **Next Review Date:** |
|  |  |  |
| **Prepared by: Donny Friday, Dir. Of Technology** | | **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:**

To define and implement a methodology for identifying the Confidentiality, Availability, and Integrity requirements for Information Systems.

**Scope and Applicability**

This policy applies to Information Systems.

**Policy Statement**

Information Systems shall be assigned classifications for Confidentiality, Availability, and Integrity based on business needs and legal requirements for sharing or restricting access to information, contingency and recovery operations, and protecting the accuracy of information.

**Procedures**

**Responsibilities**

1. The Sun Health HIPAA Security Officer is responsible for the development, implementation, maintenance, and compliance monitoring of information classifications.
2. Workforce Members are responsible for understanding, observing, and maintaining the Confidentiality of Information Systems based on its classification.
3. Appropriate controls shall be defined and implemented to conserve Confidentiality classifications of Information Systems
4. Appropriate controls shall be defined and implemented to recover and reconstitute Information Systems based on Availability classifications.

**Confidentiality Classifications**

1. All Information Systems must carry a Confidentiality classification as defined by one of the following categories:
   1. NON-SENSITIVE INFORMATION
      1. PUBLIC - Information that is available to the general public and intended for distribution outside Sun Health. This information may be freely disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, public web sites, and press releases.
      2. INTERNAL - Information that does not clearly fit into the other categorizations. The unauthorized disclosure, modification or destruction of this information is not expected to seriously or adversely impact Sun Health, its residents, patients, employees, or its business associates. Examples include the company telephone directory, new employee training materials, and internal policy manuals.
   2. SENSITIVE INFORMATION
      1. CONFIDENTIAL - Information that is intended for use within Sun Health. Its unauthorized disclosure could adversely impact Sun Health, its residents, its patients, its employees, and its business associates. Information that some people would consider private may be included in this classification. Examples include financial information, purchasing information, vendor and other business contracts.
      2. RESTRICTED - The most sensitive medical and business information that is intended strictly for use within Sun Health. Its unauthorized disclosure could seriously and adversely impact Sun Health, its residents, its patients, its employees, and its business associates. Examples include personally identifiable information (PII), protected health information (PHI), appointment schedules, and patient account records. Other examples include merger and acquisition documents, corporate level strategic plans, and attorney client privileged information.
2. When information has not been explicitly classified for Confidentiality, the information by default shall be considered as Internal.
3. When information of different Confidentiality classifications is combined, the resulting collection of information must be classified at the higher level.

**Availability Classifications**

1. All Information Systems must carry an Availability classification as defined by one of the following categories:
   1. CRITICAL - Applications and systems designated “Critical” are mission-critical, impact resident or patient care, or other key operations, and require immediate data recovery resources to ensure prompt restoration, recovery, and operability. Failure of these applications and systems to function for even a short period of time could have a severe impact on Sun Health’s ability to carry out its mission and operations.
   2. HIGH - Applications and systems designated as “High” and may impact resident or patient care, information services, finance, labor and attendance, and physical security. Failure of these applications and systems is allowable for a short period of time.
   3. MEDIUM - Applications and systems designated “Medium” and may tolerate a short period of loss of Availability.
   4. LOW - Applications and systems designated “Low” are lower priority and may tolerate a significant loss of Availability. Recovery will be initiated when normal Information Systems operations are reestablished.

**Integrity Classifications**

All Information Systems must carry an Integrity classification as defined by one of the following categories:

* 1. HIGH - Unauthorized modification or destruction of information could have a severe or catastrophic adverse effect on Sun Health operations, assets, or individuals.
  2. MEDIUM - Unauthorized modification or destruction of information could have a serious adverse effect on Sun Health operations, assets, or individuals.
  3. LOW - Unauthorized modification or destruction of information would have a limited adverse effect on Sun Health operations, assets, or individuals.

**Review and Revision**

1. Information Systems should be reviewed for possible reclassification 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.

**Definitions**

**Availability** -Means that information is accessible and useable upon demand by an authorized person.

**Confidentiality** -Means that information is not made available or disclosed to unauthorized persons or processes.

**Integrity** -Means that information is real, accurate, and safeguarded from unauthorized modification.

**Information System** -Means any 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.

**Workforce Member** -Means employees and other persons whose conduct, in the performance of work, is under the direct control of Sun Health, whether or not they are paid by Sun Health. 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 Sun Health 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 Management Process | §164.308(a)(1), §164.308(a)(1)(ii)(A), §164.308(a)(1)(ii)(B) |
| Contingency Plan | §164.308(a)(7)(ii)(E) |

**Revision History**

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

This policy is subject to the Master Service Agreement, confidential, and for internal business use only.

Nothing contained herein shall be construed as conferring by implication, estoppel or otherwise any license or other grant of right to use this customized intellectual property of BOC, except as expressly provided herein. This intellectual property was created for clients of blue orange compliance (BOC) for their sole and exclusive use. This property is not intended for the resale or reuse, except as BOC may voluntarily choose to transfer such property, in full, or in part. All customized work has a lifespan where it remains applicable for a client. BOC is not responsible for misprints, out-of-date information, technical inaccuracies, typographical or other errors appearing in this intellectual property. All information and related materials it contains are provided "AS IS", and is not intended to be legal advice. BOC makes no representation or warranty whatsoever regarding the completeness, accuracy, currency, or adequacy of, or the suitability, functionality, or availability, of the information or materials it contains. By ongoing use of this material without the availability of a current support contract from BOC, client assumes the risk that the information and materials may no longer be complete, accurate, in date, or may not meet your needs and requirements.