|  |
| --- |
| **TITLE: User Access Policy**  |
| **DEPARTMENT:** |
| **Effective Date:** | **Revised Date:** | **Next Review Date:** |
|  |  |  |
| **Prepared by: Donny Friday, Dir. Of Technology** | **Date: 9/31/21** |
| **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 establish and implement logical access controls and procedures that ensure only authorized Users can access Sun Health Information Systems that adhere to the principle of least privilege.

**Scope and Applicability**

This policy, associated procedures and guidelines apply to all Information Systems and Users.

**Policy Statement**

Logical access controls and procedures shall be established and implemented to ensure that only authorized Users, under specified conditions can access Sun Health Information Systems.

**Procedures**

**User Access**

1. All access to Information Systems (applications, software) or tool and solutions that store and transmit data etc., are subject to monitoring and logging.
2. Information Systems shall uniquely identify and authenticate Users for access to systems containing Sensitive information.
3. A provisioning process shall be implemented for establishing, activating, modifying, reviewing, disabling, and removing User accounts.
4. User Access privileges shall be allocated to individual Users or to groups, based on the minimum privileges required to fulfill the Users’ job function, according to the principle of least privilege.
5. Vendors and partners providing technical or business support services will be required to have an approved agreement such as a business associates agreement, prior to obtaining access to information and technology systems.
6. Prior to being granted access to Sun Health Information Systems, Users must sign applicable access agreements and have completed basic security awareness training.
7. Privilege escalation, the act of exploiting a bug, design flaw or configuration error to gain unauthorized access to Information System resources is prohibited ; users are required to report any such errors immediately.

**User Account Termination, Suspension, Modification, and Review**

1. Access to Sun Health Information Systems shall be disabled or removed when a User is terminated; all departments must work with the technology department to provide updated information on employment status or role changes that impacts access to information.
2. All access, including User accounts shall be disabled for Users on extended leave of absence (e.g., maternity leave, medical leave, etc.) unless specifically authorized.
3. User accounts that have been disabled for a designated period of time shall be removed unless the account has been approved for retention to address business requirements.
4. User Access shall be modified to reflect changes to a User's job function’ all departments must work with the technology department to provide updated information on employment status that impacts access to information.
5. Temporary user accounts (for testing, contractors and temporary employees) must have an appropriate expiration date, as defined by the technology team and a department leader.
6. Sun Health Information System accounts must be reviewed in accordance with audit policies and procedures.

**Log-in Procedures**

1. Authentication to Sun Health Information Systems shall require a unique User ID and password. An exception may be granted for shared workstations, such as nursing stations, treatment rooms, etc.
2. Information systems shall be configured to limit the number of unsuccessful logins and to lock out the user account after the maximum allowed unsuccessful attempts (5).

**Unattended User Equipment**

1. Users shall manually lock unattended computers.
2. Inactive computer systems shall initiate a screensaver and/or session lock after 10 minutes of inactivity. Session locks shall remain in effect until the User reestablishes access using authorized authentication procedures.
3. Operational systems that require immediate access to time-sensitive resources related to the protection to life and/or property may be granted an exemption from this requirement.

**Wireless Access**

1. Identification and authentication procedures shall be established to authorize wireless access to non-public Information Systems and Sun Health resources

**Remote Access**

1. A CAR form must be submitted and approved to access Sun Health Information Systems remotely. Access to the authorized webmail portal is exempt from this requirement.
2. Any device used to access Information Systems, including webmail, must conform to applicable security measures.
3. VPN and other remote connection tools and methods must employ appropriate security measures.

**Mobile Devices**

1. Mobile devices include, but are not limited to, laptops, smartphones, tablets, USB storage, etc.
2. Personally owned devices may not be connected to non-public, Sun Health owned wired or wireless networks.
3. Only approved USB storage devices may be utilized to store or connect to Information Systems.
4. Mobile devices that can access or store Sensitive information must be encrypted.

**Separation of Duties**

1. Appropriate divisions of responsibility and separation of duties shall be established as needed to eliminate conflicts of interest in provisioning and management of User accounts; all departments must work with the technology department to provide updated information on employment status or role changes that impacts access to information.

**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**

**Information System** -Meansany combination of 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.

**Least Privilege** - principle of minimal privilege or the principle of least authority, required to complete work.

**User Access –** Means logical access to Information Systems (network and software system accounts).

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

**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** |
| Workforce Security  | §45 CFR 164.308(a)(3)(i) |
| Authorization and/or Supervision | §45 CFR 164.308(a)(3)(ii)(A) |
| Workforce Clearance Procedure | §45 CFR 164.308(a)(3)(ii)(B) |
| Termination Procedures | §45 CFR 164.308(a)(3)(ii)(c) |
| Information Access Management | §45 CFR 164.308(a)(4)(i) |
| Health Care Clearinghouse | §45 CFR 164.308(a)(4)(ii)(A) |
| Access Authorization | §45 CFR 164.308(a)(4)(ii)(B) |
| Access Establishment and Modification | §45 CFR 164.308(a)(4)(ii)(c) |
| Log-in Monitoring | §45 CFR 164.308(a)(5)(ii)(c) |
| Workstation Use | §45 CFR 164.310(b) |
| Access Control | §45 CFR 164.312(a)(1) |
| Unique User Identification | §45 CFR 164.312(a)(2)(i) |
| Automatic Logoff | §45 CFR 164.312(a)(2)(iii) |
| Person or Entity Authentication | §45 CFR 164.312(d) |
| 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.