# Version Control

REVISION HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Responsible Party |
| 2 | 08/04/22 | Update Password and BYOD | Donny Friday |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# User access modification, deactivation and removal

|  |  |  |
| --- | --- | --- |
| Applies To | Description | Action |
| Terminated User  (Involuntary) | Account inactivation and removal. | Deactivate immediately. |
| Terminated User  (Voluntary) | Account inactivation and removal. | Deactivate within 2 business days or transfer authentication to prevent unauthorized access. |
| All Users | Account suspension for extended leave of absence | Deactivate for absence over 90 days or those directed by HR. |
| All Users | Unsuccessful logins attempts | 5 failed attempts. Lock 15 minutes |
| All Users | User accounts that have not had logins within 30 days | Deactivate for over 90 days. |
| All Users | Notification and modification of User role changes | Managers to notify within 14 days. Access changes made within 2 business days. |
| All Users | Disabled accounts | Remove after 180 days unless authorized for retention. |

# Screensaver and Automatic Session Locks

|  |  |  |  |
| --- | --- | --- | --- |
| Location / Device | Description | Screen Saver | Session Lock |
| Clinical Workstations | WOW’s and other mobile devices located in public areas. | 2 minutes | 5 minutes |
| Portable Devices | Portable devices such as laptops and tablet computers located in non-secure areas. | 5 minutes | 10 minutes |
| Nursing Stations | Workstations located at attended nursing stations. | 10 minutes | 20 minutes |
| Non-Public Areas | Computers located in non-public areas that are not physically secured. | 10 minutes | 20 minutes |
| Secure Areas | Computers located in areas that are physically secured from access by unauthorized persons. | 15 minutes | 30 minutes |

# Password Requirements

|  |  |
| --- | --- |
| Applies To | Action |
| Minimum Password Length | 15 Characters |
| Password Complexity | Be at least 15 characters in length; Contain characters from three of the following four categories: |
| Password Expiration | 365 Days |
| Disallow Password Reuse | Last 24 or never reuse |
| Lock for Failed Login Attempts | 5 Failed – 10 Minute Lock or Help Desk reset |
| Deactivation for Login Inactivity | Disable account after 90 days. |

# BYOD Security Requirements

|  |  |
| --- | --- |
| Smartphone or Tablet | Action |
| Minimum PIN Length | 4 Characters |
| Lock for Inactivity | 5 Minutes |
| Find my Device Features | Enabled |
| Encryption | Required |
| Antivirus | Required for Non IOS devices |
| Lock for Failed Login Attempts | 10 Failed – Wipe Device |
| Automatic Updates | Required |

BYOD is disallowed.

# Security Officer Responsibilities

|  |
| --- |
| Description |
| Act as the designated point of contact for HIPAA Security related matters. |
| Develop, update and implement policies and procedures as required by the HIPAA Security rule and other state and federal regulations. |
| Ensure that reasonable safeguards and security measures exist, as well as proper staff training, so that electronic Protected Health Information is maintained and is not improperly used or disclosed. |
| Oversee a security management program to identify, monitor, and mitigate threats and risks to all Information Systems. |
| Conduct periodic risk analysis of information systems and security controls. |
| Implement appropriate security controls. |
| Ensure Workforce Members receive regular security awareness training. |
| Evaluate acquisitions of Information Systems products and services for compliance with appropriate security controls. |
| Conduct regular audits of Information System events. |
| Conduct regular audits of Information Systems containing Sensitive information. |
| Maintain an inventory of all Information System components. |
| Establish and maintain availability, integrity, and confidentiality classifications for all Information Systems. |
| Develop and manage the Emergency and Contingency plans and procedures. |
| Ensure backup, recovery, and retention capabilities meet business requirements. |
| Manage security incident response procedures and investigations. |

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.