TITLE: Security Incident Response Policy		
DEPARTMENT:		
Effective Date:	**Revised Date:**	**Next Review Date:**
Prepared by:		**Date:**
Administrative Approval: Chief Executive Officer, Chief Information Officer, and Compliance Officer		
CEO:		Date:
CIO:		Date:
CO:		Date:
All other related polices/procedures/protocols:		

SEE LAST PAGE FOR REVIEW HISTORY

Purpose:
To establish and maintain Security Incident response capabilities and procedures.

Scope and Applicability
This policy applies to all Information Systems and components.

Policy Statement
Policies and procedures shall be implemented to address security incidents, including the identification of, and response to, suspected or known security incidents; mitigate, to the extent possible, harmful effects of security incidents; and document security incidents and their outcomes.

Procedures
General
1. Security Incident response capabilities shall be established and maintained to address Security Incidents, including theft, misuse of data, intrusions, hostile probes, malicious software, and malicious intent of Information Systems activities.
2. In compliance with federal, state and regulations including HIPAA, Security Incidents shall be documented and escalated as appropriate.
3. Breach risk assessment procedures shall be established and activated for Security Incidents that have the potential to result in the unauthorized disclosure of ePHI or other Sensitive information.

Roles and Responsibilities
1. The Security Officer shall be responsible to take a lead role in the response to Security Incidents, including:

   a. Ensuring compliance with this policy, and, to maintain all records of incident reports, investigations, and resolutions.
   b. Coordinating the response to Security Incidents and activating resources as appropriate.
   c. Informing management of significant Security Incidents and their potential impact.
2. Legal Counsel shall be responsible for the coordination of all communications related to external law enforcement.
3. The Communications Department shall be responsible for the coordination of all public statements regarding Security Incidents.
4. Human Resources shall assist in the investigation of Security Incidents potentially caused by Workforce Member misconduct or failure to follow policies and procedures.

Reporting of Security Incidents

1. Workforce Members shall report all potential and identified Security Incidents to their respective supervisors, the Help Desk, or a Security Officer.
2. A service ticket should immediately be opened to track a potential incident.
3. The Help Desk shall notify the Security Officer upon receipt of Security Incident reports.
4. The Chief Information Officer shall be notified of all documented Security Incidents.
5. Human Resources shall be notified of any Security Incidents suspected to have been caused by Workforce Members.
6. Reported Security Incidents shall be classified based on the potential severity of the incident.
7. Review and assessment reports shall be issued to responsible management as appropriate.

Security Incident Procedures

1. A Security Incident response team should be established to respond and manage Security Incidents, adapting to the scope and scale of each incident.
2. The Security Officer shall assign responsibility for investigation and resolution of Security Incidents to the appropriate resources.
3. The Help Desk service ticket(s) shall be used to document activities, tasks, and resolutions to Security Incidents.
4. Suspicious activity or threats shall be evaluated to determine the need to escalate the incident.
5. Immediate steps shall be taken to contain the potential impact of a Security Incident.
6. Established forensic procedures shall be followed to investigate and document Security Incidents.
7. All evidence, data or information associated with a Security Incident shall be collected, analyzed, and protected.
8. Appropriate steps shall be taken to remove or mitigate any vulnerabilities pertaining to an incident.
9. Information Systems impacted by a Security Incident shall be restored to normal operations as quickly as feasible and affected Users shall be notified of the status.
10. Periodic training, testing, review, and revision of Security Incident procedures shall be conducted.

Review and Analysis

1. All Security Incidents shall be reviewed to determine that appropriate actions and necessary reporting requirements were met during the handling of the incident.
2. The review shall identify potential impacts, evaluate effects of operational changes, identify mitigating actions, and identify additional concerns.
3. The Security Officer shall determine whether to perform additional risk analysis based on the severity and impact of the incident.

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 - Means any 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.

Workforce Member - Means employees and other persons whose conduct, in the performance of their work, is 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, volunteers, and staff from third party entities who provide services.

Security Incident - The attempted or successful unauthorized access, use, modification, destruction, or interference with Information Systems.

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 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 Incident Procedures	§164.308(a)(6)(i)
Response and Reporting	§164.308(a)(6)(ii)

Revision History

Date:	Reviewed/Revised by:	New Change	No Change	Revision(s): *State reason for revision*	Initials
		✓ Check One			

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 BlueOrange 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.