HAWAII HEALTH SYSTEMS CORPORATION "Quality Healthcare For All"	Department: Information Technology Department (ITD)	Policy No.: ITD 0132A
		Revision No.:
POLICY	Issued by: Privacy and Security Council	Effective Date: October 17, 2013
Subject: **Management of Information Security Incidents and Improvements**	Approved by: HHSC Board of Directors By: Carol A. VanCamp Its: Secretary/Treasurer	Supersedes Policy: N/A
		Page: 1 of 5

Last Review: 05/09/2013; Next Review: 05/09/2014

I. PURPOSE:

The purpose of this policy is to ensure a consistent and effective approach is applied to the management of security incidents so as to minimize damage and to ensure the continuous improvement of the HHSC security posture by learning from security incidents. This policy also ensures that when evidence is necessary, it is collected and preserved in compliance with legal requirements.

II. DEFINITIONS:

Term	Definition
Command Center	Team / area to coordinate and respond effectively to a security incident.
Industry Best Practices	A methodology that, through experience and research, has proven to reliably lead to a desired result.
Network Packet Sniffer	Computer software or computer hardware that can intercept and log traffic passing over a network or part of a network for the purpose of analyzing.
Packet Captures	Obtained formatted blocks of data.
Security Incident	Events that take place on any HHSC electronic information system that violates the confidentiality, integrity, or availability of the system and/or its data.
Stakeholder	Any person who uses HHSC Information Assets, including, but not limited to HHSC facility and corporate office employees, board members, volunteers, students, physicians, vendors, contractors, and other external parties.
Tamper-Resistant Media	A secure medium such as CD or DVD for writing and extracting data.
TCP/IP Port	Transmission Control Protocol/Internet Protocol - A number assigned to user sessions and server

	applications in a network.

III. POLICY:

1. Responsibilities and Procedures

Incidents should be reported to the Chief Information Security Officer (CISO) or the HHSC Information Security Team. The HHSC Information Security Team will consist of one or more members from the HHSC Corporate office, and one or more members from each of the HHSC Regions. The report should include all relevant information that was used to determine that an incident is occurring or has occurred.

The HHSC Information Security Team will notify the appropriate parties that an incident has occurred. The communication plan will be determined on a case-by-case basis and will contain information on the incident and a recommendation as to whether or not the Security Incident Response Team (SIRT) will be activated.

Information security incident management should be in a prioritized and coordinated manner with the SIRT and in collaboration with ITD Leadership and HHSC management.

1.1. Handling Types of Information Security Incidents

ITD personnel are to immediately secure a compromised system or device through appropriate means. This could include, but is not limited to, moving the system to a secured VLAN, physically disconnecting the system from the network, blocking a TCP/IP address or port, locking out a user account or physically securing the device.

Procedures must be formulated to handle:

- Information system failure and loss of service
- Malicious code
- Denial of service
- Errors resulting from incomplete or inaccurate data stemming from a malicious or deliberate action.
- Breaches of confidentiality and integrity
- Misuse of information system or other HHSC Information Assets.

1.2. Post-Incident Contingency Plan Review

When the investigation phase has been completed, the SIRT will recommend corrective actions to address the incident. Executive Leadership will make the final decision based on the collected evidence, risk analysis, and recommended actions. Examples of responses might be: contact law enforcement, observe activity and delay remediation to a later date, or quarantine and rebuild systems.

In addition to the normal contingency plans, procedures must be formulated to handle:

- Analysis and identification of the cause of the incident.
- Containment
- Planning and implementation of corrective action to prevent reoccurrences if necessary.
- Communication with those affected by or involved with the recovery from the incident.
- Reporting the action to the appropriate authority.

1.3. Use of Audit Trails and Evidence Collected

Evidence and audit trails should be collected for:

- Internal problem analysis.
- Evidence relating to potential civil or criminal proceedings.
- Negotiating for compensation from external service suppliers.

1.4. Recovery from Security Breaches

Procedures should include:

- Only authorized stakeholders may be allowed to correct the breach.
- All emergency actions taken are documented.
- Emergency actions are reported via the appropriate management chain.
- Timely validation of normal operations.

1.5. SIRT Activation

The CISO or the CIO or designee (e.g. ITD Director or Manager on-call) will determine whether or not the SIRT should be activated. This determination must be made within 2 hours of the initial report of the incident.

The SIRT will provide periodic incident updates to the CIO on the status of the investigation and when the investigation is closed.

2. Evidence Collection

Care must be taken during the collection of evidence of an event to ensure that the integrity of the evidence and documentation of the investigation are protected. It should be noted that the collected evidence may be used by law enforcement agencies.

- Only members of the SIRT team should collect and store evidence of the event.
- Image backups should be made of all systems involved in the event. Where feasible, the images should be written to a tamper-resistant media such as CD-ROM.
- All log files and packet captures should be copied to tamper-resistant media.
- All original pieces of evidence should be cataloged and labeled.
- Copies should be made of all evidence that will continue to be used. This includes photos, electronic media, and paper documents.
- Evidence should be obtained in a manner consistent with local, state, and federal laws.

3. Sanction of Internal Threat

Should an Information Security Breach be identified as the actions of an internal threat, relevant findings and evidence may be turned over to the HHSC Human Resources Office. The HHSC Human Resources Office may use the findings and evidence to rehabilitate or take corrective action against the internal threat in accordance with applicable collective bargaining agreements.

4. Learning from Incidents

Once an incident has ended, the SIRT should compile a report detailing the events and the actions taken and deliver it to the CISO. This report should also contain recommendations as to how to prevent similar exploits in the future

IV. APPLICABILITY:

This policy applies to all HHSC facilities and HHSC corporate office stakeholders. Compliance with this policy is mandatory. Compliance will include periodic reviews by the HHSC Information Security Team. Information Security Policy Exception Requests must be submitted in writing by relevant Management to the CISO, who will facilitate HHSC Leadership approval. Requests shall include justification and benefits attributed to such exception.

V. RESPONSIBILITIES:

Executive Leadership is responsible for authorizing the notification of law enforcement regarding security investigations; and for authorizing release of information about HHSC security events or incidents to reporting bodies, media, or public.

The CIO shares responsibility with the CISO for activating the SIRT; and for making available the Information Asset for evidence collection and security event analysis in order to minimize damage to HHSC Information Assets.

HHSC Management is responsible for working with ITD to implement controls to secure systems where a security incident has been discovered to reduce likelihood of reoccurrence of information misuse or unauthorized disclosure in future.

The HHSC Information Security Team is responsible for taking the primary lead in managing the investigation of security incidents; for notifying appropriate ITD Team for analysis of security weaknesses; for reporting to Executive ITD Leadership the outcome and recommendation on information security events; and for notifying Information Owners of reported unauthorized disclosures or misuse of Confidential Information.

ITD staff are responsible for immediately securing any compromised system or device through appropriate means, such as moving system to secured VLAN, physically disconnecting system from network, or physically securing the device in a locked room; and for cooperating in the security investigation to achieve a consistent and effective handling and containment of incident.

System Administrators are responsible for providing expert knowledge of their respective Network Operating systems to assist in analysis for incident investigation, and assist in evidence collection.

The ITD Network Team is responsible for providing technical expertise in the areas of switches, routers, and installation of network analysis tools such as network packet sniffers to actively assist in the analysis and collection of incident logs and data packets.

General Counsel is responsible for identifying liability issues and impact to the organization related to security incidents; and contacting law enforcement should it be determined that the event is a criminal matter.

Community Relations is responsible for handling all inquiries from outside the organization should a security event become public; for drafting and distribution of press releases to the public; and for managing consumer complaints regarding security incidents.

Human Resources is responsible for handling internal employee issues that may arise from security incident.

HHSC Facilities Security is responsible for providing reports of physical access to facilities if the event involved physical intrusion.

Corporate Compliance is responsible for taking necessary action to report unauthorized disclosures to the appropriate reporting authority; for initiating reporting to involved patients or customers as warranted by law; and ensuring integrity and fairness of the investigatory process so as not to prohibit disclosures required for regulatory or legislative purposes, and ensure employees protection from reprisal in accordance with laws such as the Whistleblower Protection Act (codified at 5 USC § 2302(b)(8)).

Internal Audit is responsible for auditing systems involved in security events, and for ensuring that administrative or security controls are in place to mitigate or reduce reported and discovered system security vulnerabilities.

Stakeholders are responsible for promptly notifying management of all conditions that could lead to a disruption of business activities, or any known or suspected security violations; and for cooperating with administrative security investigations.

VI. REFERENCES:

- ISO/IEC 27002:2005, an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information technology - Security techniques - Code of practice for information security management:
    - Section 13: Information Security Incident Management Objectives
        - 13.2 Manage information security incidents and improvements
- Security Standards for the Protection of Electronic Protected Health Information 45 CFR Part 164 Subpart C; 45 CFR 164.308(a)(1)(ii)(C); 45 CFR 164.308(a)(6)(i) and (ii);

VII. ATTACHMENTS: N/A

VIII. OWNERSHIP:

The CISO is responsible for all updates to the policy document. This document shall be reviewed and/or updated yearly. Change requests to this policy must be submitted in writing to the CISO. Please contact the CISO for questions or updates to this policy.