**ITD\_0131A Reporting Information Security Events and Weaknesses Policy Summary**

**Contractors and Vendors**

1. **PURPOSE:**

The purpose of this policy is to ensure information security events and weaknesses associated with information systems are communicated in a timely manner, allowing for corrective action to be taken, by establishing controls for the reporting of information security events and weaknesses.

1. **DEFINITIONS:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Security Event / Security Incident | Events that take place on any HHSC information system that violate the confidentiality, integrity or availability of the system and/or its data. |
| Sensitive Information | Information classified as Internal Use Only, Confidential, or Confidential-Reportable. |
| Stakeholder | Any person who uses HHSC Information Assets, including, but not limited to HHSC Corporate Office and facilities employees, board members, volunteers, students, physicians, vendors, contractors, and other external parties. |
| Vulnerability | A security exposure to hardware, operating system or other system software or application software component. |

1. **POLICY:**

**1. Reporting Information Security Events**

**1.1. Event Reporting**

All unusual and suspicious information-security-related events must be promptly reported to the Chief Information Security Officer (CISO) or HHSC Information Security Team. Such activities include, but are not limited to:

* Sharing user IDs and passwords and other activities that violate HHSC Information Security Policies.
* Any unauthorized loss of, or changes to, computerized production data.
* Any questionable usage of files, databases or communications networks.
* Lost or stolen (or suspected of being stolen) identification badges and physical access cards of stakeholders who have access to HHSC Secure Areas.
* Any observance or knowledge of Sensitive Information being intentionally or unintentionally discarded or left unattended.
* Transmission of Sensitive Information to unauthorized locations, to unauthorized persons or through unauthorized means.
* Positioning equipment, e.g., workstations, scanners, copiers, fax machines or printers in location or position that visitors and others can see Sensitive Information.
* Unauthorized changes and/or inappropriate modification of security controls and configuration used to protect the system and files.
* Use of physical or electronic keys by unauthorized individual to gain access to secure areas.
* Deliberate unauthorized disclosure of patient identifiable information.
* Unintentional loss or theft of a personal computer, mobile device such as a cell phone, "smart phone", or tablet that contains any HHSC information, removable media (including USB drives), or any other HHSC Information Asset.
* System, application or device malfunction that leads to or could lead to unauthorized access or compromised security controls.

**1.2. Violation and Problem Reporting Protection**

HHSC will protect stakeholders who report, in good faith, what they believe to be a violation of laws, regulations, or policies. This means that such stakeholders will not be terminated, threatened or discriminated against because they report what they perceive to be a suspected or known security breach (see HHSC Policy HR 0003 Non-Harassment Policy). Before taking any other action, these stakeholders should report the problem to their Manager, Regional or Corporate Compliance, Internal Audit, or HHSC Information Security Team, and then give the organization time to remedy the situation. Individuals seeking anonymity may contact Regional or Corporate Compliance via the Regional or Corporate Compliance Hotline (see HHSC Policy CMP 00018 Non-Retaliation and Non-Retribution).

**1.3. Reporting Security Breaches to External Parties**

If a breach or disclosure of external party information that has been entrusted to HHSC occurs, the ITD Management responsible for the information and the CISO must be immediately informed about the situation and evaluate the impact, take immediate actions to remedy the situation, and develop a communication plan to ensure the appropriate parties are notified. The relevant Business Associate Agreement, if any, shall be reviewed and followed.

**1.4. Contacting Law Enforcement**

Every decision about the involvement of law enforcement with information security incidents or problems must be made by the CISO via the affected HHSC Facility's Security Department, and in collaboration with HHSC Executive Leadership and General Counsel.

**2. Reporting Security Weaknesses**

Stakeholders should promptly report all information security alerts, warnings, suspected
or known vulnerabilities via the ITD Helpdesk, which will forward the report to ITD

Network Team and/or HHSC Information Security Team in a confidential and expeditious manner.

Stakeholders must promptly notify their HHSC Manager of all conditions that could lead to a disruption of business activities.

Unauthorized disclosures of HHSC Sensitive Information must additionally be reported to the respective HHSC Information Owners

**3. Reporting Software Malfunctions**

All apparent software malfunctions must be immediately reported to the ITD Help Desk. Vendors should be promptly and confidentially notified of information system vulnerabilities in their hardware and/or software.

1. **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 Chief Information Security Officer (CISO), who will facilitate HHSC Leadership approval. Requests shall include justification and benefits attributed to such exception.

1. **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 CISO is responsible for authorizing the investigations of security incidents or events; for directing principal ITD Staff to collect and gather evidentiary material as appropriate for the sufficiency of the review and reporting of the investigation; and for the reporting and notification to external party of HHSC violations of security involving external party.

HHSC Management is responsible for ensuring their department personnel are periodically educated on the process for reporting security incidents or events; and for conducting periodic security walk-through audits in their respective areas to monitor and identify security weaknesses.

The HHSC Information Security Team is responsible for notifying appropriate System Administrator for resolution of discovered security weaknesses; for monitoring and documenting the acceptance of risk or resolution of vulnerabilities; for education of stakeholders on process for reporting information security events; for notifying Information Owners of reported unauthorized disclosures or misuse of Sensitive Information; and for ensuring that administrative or security controls are in place to mitigate or reduce reported and discovered system security vulnerabilities.

ITD staff is responsible for reporting any security events to ITD Management as quickly as possible; for carrying out duties that may encompass being notified from stakeholders about the possible security weaknesses in systems or violations of security policy, and reporting and escalating suspected or known security concerns; and for participating in security investigations as necessary based on job role.

Corporate and Regional 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 by laws such as the Whistleblower Protection Act (codified at 5 USC § 2302(b)(8)).

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:

o Section 13: Information Security Incident Management Objectives

* 13.1 Report information security events and weaknesses
* Security Standards for the Protection of Electronic Protected Health Information 45 CFR Part 164 Subpart C; 45 CFR 164.308(a)(6)(i) and (ii)