|  |  |  |
| --- | --- | --- |
| Document ID  **ITSD108** | Title  **IT INCIDENT HANDLING** | Print Date  **mm/dd/yyyy** |
| Revision  **0.0** | Prepared By  **Preparer’s Name / Title** | Date Prepared  **mm/dd/yyyy** |
| Effective Date  **mm/dd/yyyy** | Reviewed By  **Reviewer’s Name / Title** | Date Reviewed  **mm/dd/yyyy** |
|  | Approved By  **Final Approver’s Name / Title** | Date Approved  **mm/dd/yyyy** |

**Policy:** To promptly report, investigate, and resolve all incidents that are or may be a threat to secure and effective Information Technology operations and the network.

**Purpose:** To detail policy and procedure for reporting any actual or suspected Information Technology security incident; to address security issues related to the safety, confidentiality, availability, and integrity of information maintained on the Company’s Information Technology systems.

**Scope:** This policy applies to all Company remote data terminal sites, desktop and portable computers, data centers, and telecommunications facilities, as well as all data, software, hardware, and personnel involved in information technologies.

**Responsibilities:**

The Incident Response Handling Team is responsible for investigating actual or suspected Information Technology incidents, resolving such incidents, and reporting on incident responses.

The Help Desk is responsible for reporting potential security incidents to the Information Technology Security Manager.

The Human Resources Manager is responsible for facilitating training of the Incident Response Team.

Information Technology Managers are responsible for reviewing the Information Technology Incident, reports, and their handling.

The Information Technology Security Manager is responsible for developing the Information Technology Incident Handling Plan, building an Incident Response Team, assigning incidents to the IRT for resolution, reporting incidents and responses to the Security Review Committee, and updating the Information Technology Incident Handling Plan, as needed.

The Security Review Committee is responsible for periodic review and updates and final approval of Information Technology Incident Handling. The committee should consist of the Information Technology Security Manager, Information Technology Managers, Human Resources Manager, and a member of the Help Desk.

**Definitions:** Information Technology security incident – An actual or suspected occurrence of unauthorized (intentional or unintentional) use, loss, disclosure, modification, or destruction of Information Technology hardware, software, or information.

**Procedure:**

1. **IT INCIDENT HANDLING PREPARATION** 
   1. The Information Technology Security Manager shall gather information from outside sources on Information Technology industry standards and best practices (see Additional Resources and References) in order to review and analyze the Company’s existing methods of dealing with Information Technology incidents.
   2. The Information Technology Security Manager shall present observations and findings to the Security Review Committee for comment and approval.
   3. The Information Technology Security Manager shall identify, recruit, and train technical support personnel for an Incident Response Handling Team.
      * Minimum skill/experience requirements for Team members shall be established.
      * The Incident Response Handling Team shall receive training as needed to meet or exceed skill requirements. The Information Technology Security Manager shall determine training requirements and arrange training with the Human Resources Manager.
2. **IT INCIDENT HANDLING**
   1. Any employee who has evidence of an Information Technology security incident occurring or suspects such an incident may have occurred shall notify the Information Technology Help Desk, in accordance with procedure ITTS102 IT SUPPORT CENTER, and assign an Incident ID or Trouble Ticket Number in the ITTS102-1 TECH SUPPORT LOG.
   2. The Help Desk contact shall open an ITSD108-1 IT INCIDENT REPORT and submit it to the Information Technology Manager to begin the investigation.
   3. The Information Technology Manager shall evaluate the information contained on ITSD108-1, determine the potential for loss and the risk to the Company (in accordance with ITSD101 IT THREAT ASSESSMENT), and assign the incident to the Incident Response Handling Team.
   4. The Incident Response Handling Team shall survey the incident scene, determine what information will be needed to evaluate the incident (logs, audit trails, etc.), and preserve and document evidence. The IRT shall examine and organize the evidence to facilitate analysis and reporting.
   5. The Incident Response Handling Team shall analyze the incident evidence, develop and test hypotheses regarding the incident, develop a set of findings and conclusions, and resolve the incident.
   6. The Incident Response Handling Team should perform a follow-up postmortem analysis, after an incident has been fully handled and all systems are restored to a normal mode of operation. The Team should discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s).
   7. The Team should report its findings on the open ITSD108-1 IT INCIDENT REPORT (part 2) and then send it to the Information Technology Manager for review.
3. **IT INCIDENT HANDLING REVIEW**
   1. The Information Technology Manager shall review all Incident Reports to ensure incidents are handled in a timely manner, users are satisfied with the results, and that the Company assets are protected from harm. Lessons learned, recommendations, and deficiencies should be presented to the Security Review Committee for discussion.
   2. The Security Review Committee shall review the Information Technology Incident findings on a recurring basis to determine if Incident Response Handling and the company’s security systems continue to meet Company requirements.
   3. After any review of the Information Technology Incident Handling, the Information Technology Manager shall be responsible for making appropriate changes.

**Forms:**

* ITSD108-1 IT INCIDENT REPORT

**References:**

1. **ISO/IEC 27002:2013 – INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS**

For more; see [http://www.iso.org/iso//catalogue\_detail.htm?csnumber=54533](http://www.iso.org/iso/catalogue_detail.htm?csnumber=54533).

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)**

HIPAA requires the U.S. Secretary of Health and Human Services to adopt security standards for health information. These standards are known collectively as the HIPAA Security Rule, published in 2003. The Security Rule is largely comprised of administrative safeguards (section 164.308) that require documented policies and procedures for: management of day-to-day operations; conduct and access of workforce members to electronic protected health information (EPHI); and the selection, development, and use of security controls. One of these standards pertains to policies, procedures, and processes for reporting, responding to, and managing *security incidents*.

1. **SARBANES-OXLEY ACT OF 2002**

Since its enactment by the U.S. Congress, Sarbanes-Oxley (or SOX) has required public corporations to implement internal controls over financial recordkeeping and reporting. In this era where practically every company record is electronic, a Company must have adequate internal Information Technology controls to comply with the Act.

A service desk, or help desk, must ensure that problems are recorded, investigated, and responded to in a timely and effective manner. How an organization identifies, documents, and responds to events that fall outside of normal operations – which is the purpose of the help desk – may impact financial reporting. A properly run help desk may be evidence of SOX compliance.

1. **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION #800-61 – COMPUTER SECURITY INCIDENT HANDLING GUIDE**
2. **NIST SPECIAL PUBLICATION #800-66 – INTRODUCTORY RESOURCE GUIDE FOR IMPLEMENTING HIPAA SECURITY RULE**

(See <http://csrc.nist.gov/> for a copy of documents “D” and “E,” above.)

**Additional Resources:**

1. West-Brown, Moira J., and others, Handbook For Computer Security Incident Response Teams (CSIRTs), Software Engineering Institute, Carnegie Mellon University (2nd edition, 2003) – see (<http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305>).
2. FIRST, The Forum of Incident Response and Security Teams (<http://www.first.org/>).
3. Internet Crime Complaint Center (IC3), a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) – see <http://www.ic3.gov/default.aspx>.
4. Bosworth, Kabay, & Whyne, Computer Security Handbook, 6th Ed. (Mar., 2014) – <http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118127064,subjectCdAC03.html> .

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Description of Changes** | **Requested By** |
| 0.0 | mm/dd/yyyy | Initial Release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[This page is intentionally left blank]

**ITSD108-1 IT INCIDENT REPORT**

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Security Incident ID**:

**From:** Name: Office Code:

Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_

**To:** IT Security Manager

An IT security incident was detected / observed / discovered on   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (date/time) at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (location).

**Priority** (1=low, 5=high):

**System Identification:**

System Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Software Systems Involved: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Type of Security Incident:**

The nature of this security incident was: (choose all that apply):

Unauthorized access to computing resources

Unauthorized disclosure or use of personal password

Improper use of computing resources

Alteration of data or computer systems

Other: (Explain) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Sensitivity of Data:**

Not sensitive (routine correspondence, of little or no strategic value)

Business Confidential / Proprietary Data

Business Sensitive / Financial Data

Business Sensitive / Personnel Data

Business Sensitive / Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Impact of Security Incident**

The effect of the security violation included the following: (Check all that apply)

Disclosure of data

Destruction or modification of data or systems

Denial of service

Other: (Explain on separate sheet)

**Personnel Involved:**  (List all involved personnel. Use additional sheets if required.)

|  |  |  |
| --- | --- | --- |
| **Name** | **Office Code** | **Phone** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Incident Description:** (Describe incident in detail; use separate sheets, if needed.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### ITSD108-1 IT INCIDENT RESPONSE FORM (part 2)

**Date Resolved:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Description of response to incident:**

**Time, other resources needed to respond:**

**Corrective action required:**

**Approved**

IT Manager Date

Information Security Manager Date

## FOLLOW-UP ANALYSIS

**Lessons Learned:**

**Observations/recommendations:**