SOP #_____ Revision:_____ **Prepared by:_____**
Effective Date:_____ **Approved by:_____**

Title: **ITSD108 – IT INCIDENT HANDLING**

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

Purpose: To detail policy and procedure for reporting any actual or suspected IT security incident; to address security issues related to the safety, confidentiality, availability, and integrity of information maintained on the Company's IT 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 IT incidents, resolving such incidents, and reporting on incident responses.

The Help Desk (Support Center) is responsible for reporting potential security incidents to the IT Security Manager.

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

IT Management is responsible for reviewing the IT Incident, reports, and their handling.

The IT Security Manager is responsible for developing the IT 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 IT Incident Handling Plan, as needed.

The Security Review Committee is responsible for periodic review and updates and final approval of IT Incident Handling. The committee should consist of the IT Security Manager, IT Management, Human Resources Manager, and a member of the Support Center.

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

Procedure:

1.0 IT INCIDENT HANDLING PREPARATION

1.1 The IT Security Manager shall gather information from outside sources on IT industry standards and best practices (see Additional Resources and References) in order to review and analyze the Company's existing methods of dealing with IT incidents.

1.2 The IT Security Manager shall present observations and findings to the Security Review Committee for comment and approval.

1.3 The IT 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 IT Security Manager shall determine training requirements and arrange training with the Human Resources Manager.

2.0 IT INCIDENT HANDLING

2.1 Any employee who has evidence of an IT security incident occurring or suspects such an incident may have occurred shall notify the IT Help Desk in accordance with ITTS102 IT SUPPORT CENTER and assign an Incident ID or Trouble Ticket Number in the ITTS102-1 – TECH SUPPORT LOG.

2.2 The Help Desk contact shall open an ITSD108-1 – IT INCIDENT REPORT and submit it to the IT Manager to begin the investigation.

2.3 The IT 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.

2.4 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.

2.5 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.

2.6 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).

2.7 The Team should report its findings on the open ITSD108-1 – IT INCIDENT REPORT (part 2) and then send it to the IT Manager for review

3.0 IT INCIDENT HANDLING REVIEW

3.1 The IT 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.

3.2 The Security Review Committee shall review the IT Incident findings on a recurring basis to determine if Incident Response Handling and the company's security systems continue to meet Company requirements.

3.3 After any review of the IT Incident Handling, the IT Manager shall be responsible for making appropriate changes.

Additional Resources:

A. 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://www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf).

B. FIRST, The Forum of Incident Response and Security Teams (http://www.first.org/).

C. Internet Fraud Complaint Center (IFCC), a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) – see http://www.ifccfbi.gov/index.asp.

D. Brownlee, N., and Guttman, E., Expectations For Computer Security Incident Response (RFC 2350 - BCP 21), The Internet Society, June, 1998.

E. NIST Special Publication #800-66, Introductory Resource Guide For Implementing The HIPAA Security Rule, National Institute Of Standards And Technology, March, 2005.

References:

A. ISO/IEC 17799:2005 – INFORMATION TECHNOLOGY – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, CLAUSE 6.3 (RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS)

This ISO Standard establishes general guidelines and principles for initiating, implementing, maintaining, and improving information security management within an organization. Clause 6.3 specifically addresses security incident reporting, learning from incidents, and disciplinary action.