|  |  |  |
| --- | --- | --- |
| Document ID  ITSD101 | Title  IT THREAT AND RISK ASSESSMENT | 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:** The Company shall regularly evaluate its Information Technology systems and network for threats and vulnerabilities in order to protect its Information Technology assets and reduce the Company’s risk.

**Purpose:** To describe a procedure for identifying potential threats to the Company’s information technology assets (Information Technology assets) and assessing threats on the basis of probability and risk.

**Scope:** This procedure applies to all Company Information Technology assets, including the Information Technology network.

**Responsibilities:**

The Information Technology Security Manager is responsible for conducting threat assessments of the Information Technology network and reporting on the results of such assessments. Also, the Information Technology Security Manager is responsible for continually monitoring threats and taking actions to mitigate risk to the Company’s Information Technology assets.

Information Technology Managers are responsible for evaluating the results of a threat assessment, assessing the level of risk to various Information Technology assets, and recommending actions that mitigate risk.

**Definitions:** Risk – Possibility of losing availability, integrity, or confidentiality of Information Technology assets due to a specific threat; also, the product of threat level and vulnerability level.

Threat – Expression of intent to inflict evil, injury, or damage; potential violation of security.

Threat Assessment – A process by which types of threats an Information Technology network might be vulnerable to and where the network is most vulnerable are identified.

Vulnerability – Flaw or weakness in a system’s design, implementation, or operation and management that could be exploited.

**Procedure:**

### 1.0 it THREAT & RISK ASSESSMENT – INTRODUCTION

1.1 In order to prepare for threats to its Information Technology assets and infrastructure, the Company must be aware of the types of threats that exist, the likelihood that they will occur, their potential impact, and the risk these threats may pose to the Company.

1.2 Threats may be natural or manmade. Natural threats include floods, storms, and earthquakes. Manmade threats may be accidental or intentional. Examples of manmade threats include use of unauthorized hardware or software and having unauthorized access to Company systems.

Intentional threats exist both outside the Company and within. According to one survey (see Additional Resource I), four-fifths of respondents believed the greatest threats to their organizations were internally-based.

1.3 The risk posed by any given threat is a function of the combined likelihood of the threat occurring and the impact it would have on the Company’s assets (hardware, software, data, network/infrastructure, and personnel) if it were to occur. While risk to Company Information Technology assets cannot be completely eliminated, the Company must make all reasonable efforts to minimize risk. Those efforts should begin with assessing threats and risks.

2.0 it THREAT ASSESSMENT PREPARATION

2.1 In advance of conducting a threat assessment of any of the Company’s Information Technology systems, the Information Technology Security Manager shall establish a baseline for assessment, identifying systems to be assessed (accounting, HR, sales, etc.) and determining their interconnectivity with other systems. ITAM102-5 IT ASSET INVENTORY DATABASE and ITAM102-6 IT NETWORK MAP should be used as guides.

2.2 The Information Technology Security Manager should identify and describe threats that may target the Information Technology assets and systems under consideration by one or more of the following means:

* Periodically (at least once a month) reviewing ITSD106-1 ACCESS CONTROL LOG for threat occurrences, such as unauthorized system access;
* Reviewing Information Technology incidents for trends and/or patterns, in accordance with procedure ITSD110 IT INCIDENT HANDLING;
* Reviewing any system test (test script, test procedures, expected results, etc.) for vulnerabilities testing;
* Conducting penetration testing at irregular intervals, to verify the Information Technology network’s ability to withstand intentional attempts at circumventing Information Technology security (see Additional Resource F).

2.3 The Information Technology Security Manager may acquire additional information for developing the assessment baseline by routinely reviewing threat alerts and bulletins from vendors, standards organizations, etc. Subscribing to one or more threat alert mailing lists is recommended (see Additional Resource G).

2.4 To determine if the Company needs to act on any given threat and to what extent it should act, the Information Technology Security Manager shall classify threats/ vulnerabilities should in the following manner:

* The likelihood of threats occurring, according to information provided by external sources (see Additional Resources B – D). Threat likelihood may be categorized as:

1. Low – the threat is unlikely to occur. For example, the Company’s three sites are all more than 500 miles from any ocean, so a hurricane or typhoon would not normally be a threat to the Company;
2. Medium – the threat may occur. For example, one or more of the Company’s sites is located in an earthquake zone, so an earthquake is likely to have an effect on the Company; and
3. High – the threat is likely to occur. For example, if the Company does not require password access to computers or data stores, the likelihood is high that someone will eventually access and steal or compromise Company data.
   * The impact of threats, in the absence of protection, and the possible or likely consequences of each. Threat impact may be classified as:
     1. Low – the threat may result in minimal loss of Company assets/resources;
     2. Medium – the threat may result in a significant loss of Company assets/ resources, harm the Company’s mission or interests, or result in injury to an employee; and
     3. High – the threat may result in a very costly loss of Company assets/ resources, significantly harm the Company’s mission, interests, or standing, or result in serious or fatal injury to an employee.
        + An exposure rating or risk assessment shall be based on likelihood and impact ratings. A risk matrix is prescribed (Figure 1), with likelihood running from low to high along one axis and impact running from low to high on the other axis. The resulting exposure rating/risk assessment shall be used to prioritize threats (Figure 2).
     4. High-risk threats require the highest security levels and present the greatest need for immediate action, if existing security tools and techniques are inadequate.
     5. Low-risk threats may require little or no response on the part of the Information Technology Security Manager.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Impact** | **Low** | **Medium** | **High** |
| **Likelihood** | **High** | Low | Medium | High |
| **Medium** | Low | Medium | Medium |
| **Low** | Low | Low | Low |

Figure 1 – Risk Matrix

|  |  |
| --- | --- |
| **Risk Level** | **Description and Actions** |
| **High** | Preventive actions are required and a preventive action plan shall be developed and implemented as soon as possible. |
| **Medium** | Preventive actions are required and a plan to incorporate those actions within a reasonable time frame shall be developed. |
| **Low** | IT Management should confer with managers of affected systems to determine if preventive action is required or if risk is acceptable. |

Figure 2 – Threat Priority

3.0 it THREAT/risk ASSESSMENT

3.1 At regular intervals (once every six months, at least), the Information Technology Security Manager shall conduct a threat/vulnerability scan of the Information Technology network. This scan should be performed using commercially available software designed expressly for the purpose (see Additional Resource F).

* 1. The Information Technology Security Manager shall review scan results and analyze the findings in order to determine if the Company needs to act on them and to what extent.

3.3 The Information Technology Security Manager shall create ITSD101-1 THREAT ASSESSMENT REPORT, summarizing assessment findings and containing the following information, at a minimum:

* Systems reviewed;
* Number of threats found this period and last; and
* A summary of identified threats.

3.4 The Information Technology Security Manager shall submit ITSD101-1 to Information Technology Managers and the affected systems’ management for their review. Information Technology Managers and management of the affected systems shall determine if preventive actions are required, in accordance with ITSD108 IT INCIDENT HANDLING.

**4.0 IT THREAT/RISK MANAGEMENT REVIEW**

4.1 The Information Technology Security Manager shall periodically review the risk assessment process to ensure its continued timeliness and applicability. Historical data from ITSD101-1 (i.e., number, nature, and severity of threats over time) shall help determine if risks are under control.

4.2 Any time a significant implementation, revision, etc., takes place, the Information Technology Security Manager shall review the risk assessment process, to ensure existing controls are applicable to such changes or if improved controls are required.

**Forms:**

* ITTS101-1 IT THREAT/RISK ASSESSMENT REPORT

**References:**

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

Threats to company information can come from within as well as from the outside, as incidents at Enron and WorldCom have shown. The Sarbanes-Oxley Act, passed by the U.S. Congress in 2002, was designed to prevent manipulation, loss, or destruction of publicly-held companies’ records by requiring public companies to exercise adequate internal controls. Conducting regular threat assessments helps companies comply with the requirements of the Act and makes good business sense.

**B. RISK IT FRAMEWORK FOR MANAGEMENT OF IT RELATED BUSINESS RISKS**

Detailed information can be found at <http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx>.

### C. Health Insurance Portability & Accountability Act OF 1996 (HIPAA)

The Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule) creates national standards to protect individuals’ personal health information and gives patients increased access to their medical records. As required by the Health Insurance Portability and Accountability Act (HIPAA), passed by the U.S. Congress in 1996, the Privacy Rule covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically. Most covered entities (certain health care providers, health plans, and health care clearinghouses) must comply with the Privacy Rule by April 14, 2003. Small health plans have until April 14, 2004 to comply with the Rule.

**D. NIST SPECIAL PUBLICATION #800-30, REV. 1 – GUIDE FOR CONDUCTING RISK ASSESSMENTS (SEPT. 2012)**

This publication is available at <http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf>.

**Additional Resources:**

* 1. Microsoft TechNet provides a Security Risk Management Guide online that small businesses may find helpful. This guide can be found at <http://technet.microsoft.com/en-us/library/cc163143.aspx>.
  2. SANS (SysAdmin-Audit-Network-Security) Institute – SANS is one of the largest sources for information security training and certification in the world. SANS develops, maintains, and makes available (at no cost) the largest collection of research documents about various aspects of information security and it operates the Internet’s early warning system, the Internet Storm Center. Information on SANS is available at <http://www.sans.org/about/>.
  3. The Institute of Internal Auditors (IIA) is another good source of information on tools and resources for managing security. The IIA’s web site address is <http://www.theiia.org/>.
  4. Klevinsky, Laliberte, and Gupta, Hack I.T. – Security Through Penetration Testing, Addison-Wesley, 2002.
  5. Vulnerability scan tools are readily available via the Internet; one example is the Microsoft Baseline Security Analyzer (MBSA), which may be found at <http://technet.microsoft.com/default.aspx>. A list of other vendors and their scan tools may be found at the Network Computing web site (see <http://www.nwc.com/showitem.jhtml?articleID=15000643>).
  6. Microsoft, SANS, ZDNet, and a number of other sources issue security (threat) alerts through public media and e-mail. Companies and individuals may usually subscribe to e-mail alerts at no cost to them. It is strongly recommended that the Company subscribe to at least one e-mail alert list.
  7. Power, Richard, “1999 CSI/FBI Computer Crime and Security Survey,” *Computer Security Issues & Trends*, Computer Security Institute, Winter, 1999.

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Description of Changes** | **Requested By** |
| 0 | mm/dd/yyyy | Initial Release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[This page intentionally left blank]

**ITSD101-1 IT THREAT/RISK ASSESSMENT REPORT**

Date:

Systems Reviewed:

Threats found this period:

Description:

Threats found last period:

Description:

Threat Summary:

|  |  |  |
| --- | --- | --- |
| **Risk Level** | **Number** | **Description** |
| LOW |  |  |
| MEDIUM |  |  |
| HIGH |  |  |

IT Security Manager:

[This page intentionally left blank]