|  |  |  |
| --- | --- | --- |
| Document ID  **ITAM104** | Title  **IT ASSET 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 assess (evaluate) its Information Technology assets for conformance to Company requirements.

**Purpose:** To identify hardware and software (Information Technology assets) on the Company Information Technology network, determine if those assets are appropriate for the Company’s needs, determine if these assets are properly licensed and versioned, and if they conform to Company standards.

**Scope:** All Information Technology assets that make up the Company’s Information Technology system/network are subject to this procedure.

**Responsibilities:**

The Information Technology Asset Manager is responsible for supervising the Information Technology asset assessment program.

The Tech Support Manager is responsible for conducting complete, detailed, and objective Information Technology asset assessments, writing nonconformance reports, and reporting findings of Information Technology asset assessments.

**Definitions:** Network scan (or scan) – Scanning an Information Technology network (with specialized software) to confirm the presence or absence of computer hardware or software, check asset configurations, verify software versions, manage software licenses, track lease and warranty information, detect network vulnerabilities, etc. Commercial and open source software for conducting Information Technology asset scans is readily available; see Additional Resource A for guidance.

Information Technology Asset – Any computer hardware, software, Information Technology-based Company information, related documentation, licenses, contracts or other agreements, etc. In this context, Information Technology assets may be referred to as just “assets”.

Nonconformance – A significant, material failure to conform to one or more requirements; also referred to as a “nonconformity”. Moving a PC from one desk/user to another without the knowledge or permission of the Information Technology Asset Manager is one example of a nonconformance.

**Procedure:**

### 1.0 IT asset assessment PLAN

1.1 Information Technology asset assessments shall be conducted at regular intervals. Assessments should be conducted annually, at a minimum. (See Reference A.)

* Information Technology asset assessments should also be conducted whenever a large turnover of assets (for example, a large number of PC leases expires in a short time frame) occurs.

1.2 Prior to an assessment, the Information Technology Asset Manager shall review ITAM104-1 IT ASSET ASSESSMENT CHECKLIST for possible modifications. This checklist shall be used by the Tech Support Manager as a guide to conducting Information Technology asset assessments.

### 2.0 IT Asset SCAN

2.1 The Information Technology Asset Manager shall ensure that the Tech Support Manager has the current version of the following on hand prior to conducting a network scan:

* ITAM102-5 IT ASSET INVENTORY DATABASE;
* ITAM102-6 IT NETWORK MAP; and
* ITAM104-1 IT ASSET ASSESSMENT CHECKLIST.
  1. the Tech Support Manager shall run a scan on the Company’s Information Technology network to determine the status of all Information Technology assets on the network and compare the results with the documents listed in 2.1, looking for information such as:
* What Information Technology hardware is on the network and who are the registered “owners”;
* Whether hardware is in use or not;
* What software is installed on each computer, whether it is the correct version, and whether it is a licensed copy; and/or
* Whether unapproved/unauthorized software has been installed on any PC.

2.3 If a nonconformance is found, the Tech Support Manager shall report it in accordance with procedure ITSD109 IT INCIDENT HANDLING.

### 3.0 DOCUMENTATION AND DISTRIBUTION

3.1 The Tech Support Manager shall consolidate and summarize asset scan results on ITAM104-2 IT ASSET SCAN SUMMARY.

3.2 The Tech Support Manager shall prepare and submit their findings – including forms ITAM104-1 and ITAM104-2 – to the Information Technology Asset Manager.

### 4.0 NONCONFORMANCE HANDLING

4.1 If a nonconformance is discovered in the course of an asset assessment, the Information Technology Asset Manager shall write a Corrective Action Request (CAR), in accordance with procedure ITSD109 IT INCIDENT HANDLING.

4.2 The CAR shall be submitted to the Manager of the department where the nonconformance occurred.

4.3 The Department Manager receiving the CAR shall submit a reply in accordance with procedure ITSD109 IT INCIDENT HANDLING.

4.4 If a corrective action was taken, the Information Technology Asset Manager should review the situation within three months to verify that the corrective action was effective.

### 5.0 IT ASSET Records update

After the Information Technology asset assessment and subsequent corrective actions, The Information Technology Asset Manager shall ensure timely and accurate updates to ITAM102-5 IT ASSET INVENTORY DATABASE and ITAM102-6 IT NETWORK MAP. (See Reference B.)

**Forms:**

* ITAM104-1 IT ASSET ASSESSMENT CHECKLIST
* ITAM104-2 IT ASSET SCAN SUMMARY

**References:**

1. **ISO STANDARD 27002:2013 – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, CLAUSE 8 ASSET MANAGEMENT**

Clause 8 of the Standard is the Asset Management standard, which deals with asset accountability and information classification.

ISO Standard 27002:2011 and its companion standards, ISO 27001:2011 and ISO 27005:2008, provide a comprehensive set of controls comprising best practices in the field of information security.

ISO 27002 was formerly known to ISO as “17799” and may continue to be known that way in the business and Information Technology world for some time. See <http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm>

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

Sarbanes-Oxley, passed by the U.S. Congress in 2002, is designed to prevent manipulation, loss, or destruction of records within publicly-held companies doing business in the U.S. Because virtually all companies keep records electronically, Section 404 of the Act implies that “an adequate internal control structure” is Information Technology-based.

Therefore, regular scanning of the Company’s Information Technology network, evidence of regular scanning, and keeping an up-to-date Information Technology asset inventory are all evidence of adequate internal controls.

**Additional Resources:**

1. There are many types of scans that may be conducted on a computer network – hardware scans, software scans, wireless and wired network scans, security scans, etc. System Center 2012 R2 Configuration Manager (<http://www.microsoft.com/en-us/server-cloud/products/system-center/2012-r2-configuration-manager/default.aspx#fbid=Xd6tQVcmWsT>) is one form of asset management software. Additional asset management software providers and their products may be found by searching the Internet.

**Revision History:**

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

**ITAM104-1 IT ASSET ASSESSMENT CHECKLIST**

Assessment #: Date:

Area Evaluated:

Dept. Mgr.:

Lead Assessor:

Assessor:

**IT Asset Accountability** **Response and Comments**

1. Is every IT asset – hardware, software, and related documentation – accounted for?
2. Is an IT asset inventory maintained?
3. Is an IT asset classification scheme in place?
4. Does the inventory identify the owner and location of each asset?
5. Does the company have a clear set of standards for IT assets? Are the standards up to date? How often are they reviewed? Do they conform to industry standards and/or legal requirements?
6. Is the IT asset inventory reviewed regularly to see the company does not risk having obsolete IT assets in inventory?
7. Does every hardware asset conform to company standards? Are they clearly and properly identified?
8. Do all software assets conform to company standards? Are they clearly and properly identified?
9. Does the IT asset inventory thoroughly and accurately account for software versions and licenses?
10. Is there an IT network diagram? Is it accurate? Is it readily produced? When was it last reviewed? How frequently is it reviewed?

**Tech Support Area** **Response and Comments**

1. Are workers organized and scheduled?
2. Are adequate working areas provided for tasks?
3. Are drawings and schematics organized, inventoried and readily accessible?
4. Are work instructions sufficient?
5. Are all items (new hardware/software, items being repaired, etc.) inventoried?
6. Is there any obvious disorganization?

* Tools randomly scattered about?
* Parts on benches disorganized?
* Components or parts for other assemblies present?

1. Are work areas (benches) clean?
2. Are parts organized and stored efficiently? Are stores clearly marked?
3. Are staging areas organized?

**Tech Support Equipment** **Response and Comments**

* 1. Are tools properly inventoried? Are records accurate and up-to-date?
  2. Are tools properly stored when not in use?
  3. Are tools in good working order?
  4. Are tools requiring calibration being recalibrated on a regular basis? Are calibration records current?

**Tech Support Records** **Response and Comments**

* + 1. Are production records (installations, repairs, etc.) maintained? Are they complete and up-to-date? Are they readily accessible?
    2. Are “work pending” and “work in process” records included with the above? Are they likewise complete and up-to-date? Are they also readily accessible?

**User Complaints** **Response and Comments**

1. Is there a log of user complaints and concerns? Is it complete, up to date, organized, and readily accessible?
2. What is the level of detail in the log file? Are complaints/concerns classified clearly and logically?
3. Is this “complaint file” periodically reviewed for trends?

**Authorization**

Comments:

Tech Support: Date:

IT Asset Manager: Date:

[This page intentionally left blank]

**ITAM104-2 IT ASSET SCAN SUMMARY**

(Attach results from scanning software to this sheet.)

**Hardware scan results:**

**Software scan results:**

**Nonconformities (discrepancies) found:**

**Other comments:**

Tech Support: Date:

IT Asset Mgr.: Date:

[This page intentionally left blank]