|  |  |  |
| --- | --- | --- |
| Document ID  ITSD107 | Title  IT SECURITY AUDITS | 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 conduct periodic audits of Information Technology Security functions, processes, and procedures.

**Purpose:** To ensure that the Company’s Information Technology security system conforms to legal, regulatory and Company requirements, that the system is effectively implemented and maintained, and that it performs as expected.

**Scope:** This applies to all Information Technology systems and assets.

**Responsibilities:**

Information Technology Managers are responsible for attending opening and closing meetings regarding the Information Technology Security audit, reviewing audit findings, and for final approval of the audit report.

The Audit Team Leader is responsible for: conducting and supervising the Information Technology Security audit; supervising audit team members, if any; conducting opening and closing meetings for the audit; preparing and presenting the final audit report.

The Information Technology Security Manager is responsible for reviewing findings of the Information Technology Security audit and overseeing corrective actions, if any.

Information Technology staff are responsible for complying with the Information Technology Security audit while in process and providing assistance to the security auditor, when needed.

**Definitions:** Audit criteria – Policies, practices, procedures, or requirements against which the auditor compares collected audit evidence about the subject matter.

Audit evidence – Records, statements of fact, and other information that are relevant to the audit criteria and verifiable.

Auditee – Party or parties whose processes, procedures, etc., are the subject of an audit.

Security audit – An examination of a computer system for security problems and vulnerabilities.

**Procedure:**

1.0 IT SECURITY AUDIT PLANNING

1.1 The Company shall conduct internal audits of its security management system at planned intervals (annually, at a minimum) to determine if its control objectives, controls, processes, and procedures conform to legal/regulatory and Company information security requirements; are effectively implemented and maintained; and perform as expected.

1.2 Information Technology Managers shall conduct an assessment of the existing Information Technology security system, in order to establish a baseline for auditing. Information Technology Managers shall report the results of this assessment to the Security Review Committee for review.

1.3 Information Technology Managers shall acquire and review additional pertinent information for Information Technology Security auditing, including applicable standards (see References A and B) and Information Technology industry standards and practices. This information shall also be shared with the Security Review Committee.

1.4 Information Technology Managers shall develop (or assign responsibility for development of) the Information Technology Security Audit Plan and submit the Plan to The Security Review Committee. The Security Review Committee shall review the Plan and may recommend changes.

1.5 Information Technology Managers shall incorporate changes into the Plan and submit it to the SRC for final review and approval.

1.6 The Plan shall serve as the basis for internal audits of Information Technology Security.

2.0 IT SECURITY AUDIt PLAN

2.1 Prior to conducting the audit, Information Technology Managers shall define the objectives, scope, and criteria of the audit; determine if the audit is feasible, and (if the audit is deemed feasible); appoint an audit team leader, who shall be required to meet minimum competency requirements for the position (see Reference B).

The audit team leader shall select an audit team, who shall be required to meet minimum competency requirements (Reference B), and shall establish contact with the Information Technology Security Manager.

2.2 The audit team leader shall conduct and/or supervise a review of Information Technology Security documentation.

2.3 The audit team leader shall prepare for onsite audit activity by preparing the audit plan (using ITSD107-3 IT SECURITY AUDIT PLAN as a guide) and assigning tasks to members of the audit team.

Audit team members shall prepare work documents, such as audit checklists, sampling plans, and forms for recording information (minutes of meetings, supporting evidence, audit findings, etc.).

2.4 The audit team shall conduct the onsite audit, which shall consist of:

* The audit team leader conducting an opening meeting with Information Technology Managers and the Information Technology Security Manager to confirm the audit plan (including roles and responsibilities of all parties), explain how audit activities will occur, confirm lines of communication during the audit, and provide the Auditee with an opportunity for feedback.
* Communication during the audit.

1. The audit team should meet periodically to exchange information, assess the progress of the audit, and reassign work between members, if needed.
2. The audit team leader should periodically (depends on the scope of the audit) communicate audit progress and any concerns to the Information Technology Security Manager.
3. Evidence that suggests an immediate and significant risk should be reported to the Information Technology Security Manager immediately.
4. Audit team members’ concerns about issues outside the audit scope should be reported to the audit team member for possible communication to the Information Technology Security Manager.

* Audit team members shall collect, record, and verify information relevant to the objectives, scope, and criteria of the audit. Information may be acquired through interviews, observation of activities, and document reviews.
* Audit team members shall evaluate audit evidence against audit criteria and generate audit findings, which may indicate conformity or nonconformity with the criteria.

1. Conformity with audit criteria should be summarized, indicating locations, functions, or processes that were audited.
2. Nonconformities and supporting evidence should be recorded (ITSD107-2 IT NONCONFORMITY REPORT) and reviewed with the Information Technology Security Manager, to obtain acknowledgement of evidential accuracy and ensure that nonconformities are understood.
3. The audit team shall meet as needed to review their findings.

* The audit team shall confer prior to conducting an audit closing meeting to:

1. Review their findings against audit objectives;
2. Come to an agreement on the audit conclusions;
3. To prepare recommendations, if this is specified by the audit objectives; and
4. To discuss audit follow-up, if it is included in the audit plan.

* The audit team leader shall conduct a closing meeting in order to formally present the audit team’s findings and conclusions, to verify the understanding and obtain the acknowledgement of the Information Technology Security Manager, and if nonconformities are found, to agree on a timeframe for the Information Technology Security Manager to present a corrective and preventive action plan.

2.5 The audit team shall prepare, approve, and distribute ITSD107-1 IT SECURITY AUDIT REPORT.

* The audit team leader shall be responsible for preparing ITSD107-1 and for its contents.
* The audit report should provide a complete, accurate, clear, and concise record of the audit and should include or refer to the following:

1. Audit objectives and scope;
2. Where and when the audit was conducted;
3. Who took part in the audit;
4. The audit criteria; and
5. Audit findings and conclusions.

* The audit team leader and Information Technology Security Manager shall approve ITSD107-1, which shall then be distributed to persons designated by the Information Technology Security Manager.

3.0 IT SECURITY AUDIT REVIEW

3.1 The Information Technology Security Manager shall meet with Information Technology Managers to review ITSD107-1 (and ITSD107-2, if one has been generated) and plan to take corrective actions, if required.

3.2 If it has been decided to take corrective action, the Information Technology Security Manager shall submit a corrective action plan, including objectives, actions, and deadlines, to the audit team leader. If it has been decided not to take corrective action, the Information Technology Security Manager shall inform the audit team leader of this decision, with explanation.

**4.0 IT SECURITY AUDIT – CORRECTIVE ACTION**

4.1 The Information Technology Security Manager shall be responsible for taking corrective actions, if required. Corrective actions shall be taken within the period prescribed in audit and as agreed to by the Information Technology Security Manager.

4.2 The Information Technology Security Manager shall notify the audit team leader when corrective actions have been completed. The audit team leader shall verify that corrective actions have been taken and that they are having the desired effect.

**Forms:**

* ITSD107-1 IT SECURITY AUDIT REPORT
* ITSD107-2 IT NONCONFORMITY REPORT
* ITSD107-3 IT SECURITY AUDIT PLAN

**References:**

**A. ISO/IEC 27001:2013 INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS- REQUIREMENTS**

**Additional Resources:**

1. SANS (**S**ysAdmin-**A**udit-**N**etwork-**S**ecurity) Institute, found at <http://www.sans.org>.
2. The Information Systems Audit and Control Association (ISACA), located at <http://www.isaca.org/>.

**Revision History:**

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

[This page intentionally left blank]

**ITSD107-1 IT SECURITY AUDIT REPORT**

* 1. **Audit Objectives**
  2. **Audit Scope**
  3. **Audit Client**

IT Security Manager

* 1. **Audit Team (leader and members)**
  2. **Dates And Locations Of Onsite Audit**
  3. **Audit Criteria**
  4. **Audit Findings**
  5. **Audit Conclusions**

Audit Team Leader: Date:

IT Security Manager: Date:

[This page intentionally left blank]

**ITSD107-2 IT NONCONFORMITY REPORT**

**Date:**

**Auditor:**

**Area / System:**

**Description of nonconformity:**

**Supporting evidence:**

[This page intentionally left blank]

**ITSD107-3 IT SECURITY AUDIT PLAN**

* 1. **Audit Objectives:**
  2. **Audit Criteria:**
  3. **Audit Scope:**
  4. **Dates and Locations of Audit:**
  5. **Estimated Time and Duration of Onsite Audit Activities:**
  6. **Roles and Responsibilities of Audit Team Members:**
  7. **Resources Required to Conduct Audit:**
  8. **Auditee Representative:**
  9. **Audit Report Topics:**
  10. **Logistical Arrangements (travel, etc.):**
  11. **Confidentiality Matters:**
  12. **Other:**

[This page intentionally left blank]