|  |  |  |
| --- | --- | --- |
| Document ID  **ITTS102** | Title  **IT SUPPORT CENTER** | 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 have an Information Technology Support Center, to provide ongoing emergency and non-emergency technology support to all departments and users.

**Purpose:** To identify staffing, training, and logistic requirements for an internal service/support center; to provide cost-effective staffing, training, and logistics for an effective support department.

**Scope:** This procedure applies, in particular, to the Information Technology Support Center. In general, all departments within the Company have technology needs, including:

Hardware support – Assistance with installation, usage, upgrades, or failures of all Information Technology related computer and communication equipment;

Software support – Assistance with technical questions on all operating systems, e-mail, applications, and database software; and

Telecommunications – Assistance with telephone, voice mail, pager, and all wireless equipment, including all setup, usage, and hardware difficulties.

Therefore this procedure, while not directly applicable to other departments, has a direct impact on the ability of every other department to do business in a manner that satisfies Company and customer requirements.

**Responsibilities:**

Information Technology Managers are responsible for developing Support Center goals, identifying needs, developing the Information Technology Support Plan, providing resources for the Information Technology Support Center, reviewing Support Center metrics with the Support Center Manager, and recommending changes to the Plan.

The Information Technology Support Center Manager is responsible for administering the Support Center budget and other recordkeeping, recording and analyzing Support Center metrics and reporting on such metrics and other Support Center activities to Information Technology Managers on a regular basis, managing a staff of (in-house or outsourced) Technical Support analysts, recommending improvements to Information Technology Managers; and meeting or exceeding user expectations for the Support Center.

The Tech Support Manager is responsible for carrying out the daily operations of the Information Technology Support Center (i.e., delivering user support).

The Technology Review Committee is responsible for reviewing the Information Technology Support Plan, recommending revisions to the Plan, and for final approval of the Plan. The Technology Review Committee shall consist of Information Technology Managers (who shall chair the Committee) and management of the Company’s functional departments or their representatives.

**Definitions:** Technical Support (or “Tech Support”) – Provision of human resource and contract services for the installation, setup, and efficient operation of information technologies; also refers to personnel having responsibility for providing technical support.

Help Desk – Alternate name for technical support services.

**Procedure:**

### **1.0 IT SUPPORT CENTER OVERVIEW**

1.1 Information Technology Managers shall determine the requirements for the Support Center by reviewing and analyzing such information as:

* Information Technology industry standards and best practices;
* Existing Company records – formal and informal – of instances where technical support was required, including descriptions, analyses, actions taken, personnel involved, dates, and outcomes; and
* ITAD110-2 – USER SATISFACTION SURVEY.

1.2 Information Technology Managers shall determine if the Company’s needs are best met by operating and staffing the Support Center internally or by outsourcing, by:

* Measuring workload history and analyzing for trends; and
* Measuring and comparing the “total value” of each alternative to the Company.

1.3 Information Technology Managers shall develop an Information Technology Support Plan that integrates the Support Center into ITAD101-1 – INFORMATION TECHNOLOGY PLAN and ensures that the Support Center is accessible to the Company’s computer network users. The Support Plan shall include guidelines and procedures for measuring response rates, priority levels, staffing requirements, customer satisfaction, and summary reports. Information Technology Managers shall submit the Information Technology Support Plan to the Technology Review Committee for input and approval.

1.4 When the Information Technology Support Plan has been approved, Information Technology Managers shall secure resources needed to implement the Plan on an ongoing basis, in accordance with ITAD109 IT OUTSOURCING.

### **2.0 IT SUPPORT CENTER OPERATIONS**

2.1 Set up and maintain user accounts – As people enter the Company workforce, the Support Center will assign each new employee a unique identity within the Company’s computer network and assign certain data and personnel access rights and privileges. Thereafter, the Support Center will ensure that user accounts are current.

2.2 User instruction/information – The Support Center should provide information on the Company’s network and related services. The Support Center should ensure that new users are familiar with the current state of the network and the resources that are available by conducting brief introductory seminars and/or providing an introduction to network services in written form, in accordance with ITTS101 IT TRAINING PLAN. The Support Center should disseminate new and useful information on the computer network to all users as it becomes available or when needed.

2.3 Acquire and maintain computer equipment – The Support Center should install, relocate, or remove computer hardware (and related software) to/from the Company’s computer network, in accordance with ITAM102 IT ASSET MANAGEMENT.

2.4 Provide software support – The Support Center should install and maintain all applications software users need to perform his/her job efficiently and effectively, ensuring that the latest version is installed, that a site license is available and updates (patches, etc.) are disseminated in a timely and orderly fashion; again, in accordance with ITAM102 IT ASSET MANAGEMENT.

2.5 Ad hoc problem solving – The Support Center operates a “help desk” to assist computer and network users at every level with any computer-related problems they may encounter. The help desk should categorize and prioritize user problems so that Support Center resources are assigned appropriately. The Help Desk contact shall:

* Identify, categorize, and assign an Incident ID or Trouble Ticket number and complete ITTS102-1 TECH SUPPORT LOG.
* Attempt to resolve the issue, in accordance with ITTS104 IT TROUBLESHOOTING. If the issue is resolved in this manner, close the entry in ITTS102-1; otherwise:
  1. Record **unresolved** user issues/problems on ITSD108-1 IT INCIDENT REPORT and forward to Information Technology Managers for resolution, in accordance with ITSD108 IT INCIDENT HANDLING.
  2. Acknowledge receipt of **unresolved** user issues/problems immediately, using ITTS102-2 SYSTEM TROUBLE REPORT ACKNOWLEDGEMENT, submitting one copy each to the user and to Information Technology Managers.

2.6 The Information Technology Support Center Manager shall prepare a weekly report based on ITTS102-1 TECH SUPPORT LOG, listing Trouble Reports that occurred in the last week and categorizing by nature and severity. The weekly report shall be submitted to Information Technology Managers, which shall use to help allocate resources and plan the workload accordingly.

2.7 Load planning – The Support Center will monitor its activities and regularly report to Information Technology Managers. Information Technology Managers will analyze Support Center activity data to ensure continued, adequate support resources and adjust the Company’s Technology Plan, as needed.

2.8 Training plans/goals for tech support personnel – Information Technology Managers will ensure that Support Center personnel are adequately trained to perform computer network support duties and that they maintain adequate training and certification levels. (See procedure ITTS101 IT TRAINING PLAN.)

**3.0 IT SUPPORT REVIEW**

3.1 Information Technology Managers shall periodically (at least monthly) review Tech Support Logs, user satisfaction surveys, and other sources of information, analyze the data on response times and satisfaction levels, and identify issues and trends. Information Technology Managers shall report its findings and observations to the Technology Review Committee. The Technology Review Committee shall review Information Technology Managers’ findings and observations and possibly make change recommendations.

3.2 The Support Center shall be subjected to a periodic audit (once every two years, at a minimum), to verify that the Plan is clear and actionable and continues to meet Company requirements.

**Forms:**

* ITTS102-1 TECH SUPPORT LOG
* ITTS102-2 SYSTEM TROUBLE ACKNOWLEDGEMENT FORM

**Additional Resources:**

1. Help Desk Institute (HDI) (<http://www.thinkhdi.com/>).
2. Association of Support Professionals (ASP) (<http://www.asponline.com>).
3. ITSW110 SOFTWARE SUPPORT
4. ITSD108 IT INCIDENT HANDLING
5. ITTS104 IT TROUBLESHOOTING
6. ITTS105 IT USER/STAFF TRAINING PLAN

**Revision History:**

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

[This page intentionally left blank]

**ITTS102-1 TECH SUPPORT LOG**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Incident ID** | **Date-Time** | **Location** | **Problem Description** | **Problem Category** | **Severity Level** | **Problem Logged By (ID)** | **Problem Assigned To (ID)** | **Resolution** | **Resolved (Date)** | **Hours Logged** | **User Comments** | **Comment Code** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

[This page intentionally left blank]

#### ITTS102-2 SYSTEM TROUBLE ACKNOWLEDGEMENT FORM

**A. INCIDENT ID:**

**B. USER IDENTIFICATION:**

From: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Dept: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**C. SYSTEM IDENTIFICATION:**

Property ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Serial Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**D. PROBLEM CATEGORY:**

Date Received: \_\_\_\_\_\_\_\_\_\_\_\_ Date problem first noted: \_\_\_\_\_\_\_\_\_\_\_

Type of Problem: (Check One)  
 Hardware: \_\_\_\_\_\_ Software: \_\_\_\_\_\_\_ Security: \_\_\_\_\_\_\_ (See H. on back)

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

**E. DESCRIPTION OF PROBLEM:**

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

**F. EXPECTED TIME TO RESOLVE:**

**G. IF QUESTIONS, CONTACT:**

**H. SECURITY INCIDENT GUIDE:**

* 1. A system alarm or similar indication from an intrusion detection tool
  2. Suspicious entries in system or network accounting (e.g., a UNIX user obtains root access without going through the normal sequence necessary to obtain this access)
  3. Accounting discrepancies (e.g., someone notices an 18-minute gap in the accounting log in which no entries whatsoever appear)
  4. Unsuccessful logon attempts
  5. Unexplained, new user accounts
  6. Unexplained, new files or unfamiliar file names
  7. Unexplained modifications to file lengths and/or dates, especially in system executable files
  8. Unexplained attempts to write to system files or changes in system files
  9. Unexplained modification or deletion of data
  10. Denial of service or inability of one or more users to login to an account
  11. System crash
  12. Poor system performance
  13. Unauthorized operation of a program or sniffer device to capture network traffic
  14. “Door knob rattling” (e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts)
  15. Unusual time of usage (remember, more security incidents occur during non-working hours than any other time)
  16. An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user
  17. Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)

Observing one or more of these symptoms should prompt you to investigate events more closely. Work with other personnel at the Company that possess the appropriate technical and computer security knowledge to determine exactly what has occurred, if necessary.