|  |  |  |
| --- | --- | --- |
| Document ID  ITSD102 | Title  IT SECURITY PLAN | 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 protect the confidentiality and integrity of Company information while maintaining appropriate levels of accessibility.

**Purpose:** To provide an overview of the security requirements of the Company’s Information Technology system and network, to describe the controls in place or planned for to meet those requirements, and to delineate responsibilities and expected behavior of all individuals who access the system.

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

**Responsibilities:**

The Information Technology Security Manager is responsible for preparing and developing the Information Technology Security Plan and implementation schedule, implementing the Plan and any updates, and monitoring and periodic reporting on the Plan.

Information Technology Managers are responsible for establishing and periodically convening the Security Review Committee, advising the Information Technology Security Manager regarding development of the Plan, coordinating with Human Resources Management to provide user training, and verifying implementation of updates to the Plan.

The Security Review Committee is responsible for periodic review and updates and for final approval of the Information Technology Security Plan.

**Definitions:** Security - The state of being free from danger or injury. The effort to create a secure computing platform, designed so that agents (users or programs) can only perform actions that have been allowed.

**Procedure:**

1. PREPARING THE IT SECURITY PLAN
   1. The Information Technology Security Manager shall begin the planning process with an up-to-date inventory of Information Technology assets, in accordance with procedure ITAM104 IT ASSET ASSESSMENT.
   2. The Information Technology Security Manager shall continue the planning process with an assessment of threats and risks to the Information Technology system/network, in accordance with procedure ITSD101 IT THREAT ASSESSMENT.
   3. The Information Technology Security Manager shall conduct a security assessment of the Company’s Information Technology network, using ITSD102-1 IT SECURITY ASSESSMENT CHECKLIST as a guide.
   4. A Security Review Committee, consisting of Information Technology Managers, the Information Technology Security Manager, and management from the various Company departments (Human Resources, Accounting, Production, Sales, etc.), shall be established.
   5. The Information Technology Security Manager shall evaluate findings and discuss recommendations to correct deficiencies and/or improve security with the Security Review Committee.

**2.0 DEVELOPING the it security plan**

2.1 The Information Technology Security Manager shall develop the Information Technology Security Plan with assistance from Information Technology Managers, using ITSD102-2 IT SECURITY PLAN as a guide.

2.2 The Information Technology Security Manager shall ensure that the plan is comprehensive and complete and shall present the Plan and an implementation schedule (see ITSD102-3 IT SECURITY PLAN IMPLEMENTATION SCHEDULE for guidance) to the Security Review Committee for its approval.

3.0 IMPLEMENTING THE IT SECURITY PLAN

3.1 All Information Technology systems shall be identified according to a standard format. Systems identification shall include, but not necessarily be limited to, the following:

* System name and ID;
* Responsible organization(s);
* Contact information;
* Operational status;
* Description & purpose;
* Interconnections and information sharing;
* Applicable regulations; and
* Information sensitivity.

3.2 Management controls for every system shall include, but not necessarily be limited to:

* Risk assessment and management;
* Review of security controls;
* Security planning throughout the system life cycle; and
* Processing authorization.

3.3 Operational controls for each system shall include, but not necessarily be limited to:

* Personnel security;
* Physical/environmental protections;
* Production and input/output controls;
* Contingency planning;
* Hardware/software maintenance controls;
* Integrity controls;
* System documentation;
* Security awareness and training; and
* Incident response.

3.4 Technical controls for each system shall include, but not necessarily be limited to:

* Identification and authentication of users;
* Access control; and
* Audit trails.

3.5 The Information Technology Security Manager shall communicate the Information Technology Security Plan to all affected persons, distributing the plan to all managers and supervisors, requiring managers and supervisors to communicate the Plan to their staff, and resolving any questions related to the Plan.

3.6 Information Technology Managers shall coordinate employee security training with Human Resources Management. Human Resources shall train all new users in Information Technology security within one week of their hiring and retrain all users in the Information Technology Security Plan at least once every two years.

4.0 it security plan REVIEW

4.1 The Information Technology Security Manager shall routinely monitor and periodically report (once a quarter, depending on the size of the Company and its Information Technology network) to Information Technology Managers on the status of the Information Technology Security Plan.

* Any significant deviation from the Information Technology Security Plan shall require that Information Technology Managers convene the Security Review Committee to consider if changes to the Plan are required. (An example of significant deviation may be a change at the Information Technology Security Manager position, or a change in risk assessment or other security methodologies.)

4.2 Once the Security Plan is implemented, The Information Technology Security Manager shall conduct a periodic internal review of the Plan with the Security Review Committee. This review should take place at least annually and shall include an examination of:

* Current security conditions;
* Changes to the Plan, as recommended by The Information Technology Security Manager;
* User satisfaction, in accordance with ITAD110 IT DEPARTMENT SATISFACTION;
* Results of any internal or external audits, in accordance with ITSD107 IT SECURITY AUDITS; and
* Progress of the stated goals of the existing Plan.

4.3 At least once every three years, the Company shall participate in an external review (audit), to verify its compliance with the Information Technology Security Plan and help evaluate the Plan’s effectiveness.

**5.0 IT SECURITY PLAN UPDATE**

5.1 After any review of the Information Technology Security Plan, the Information Technology Security Manager shall be responsible for implementing required updates.

5.2 Within three months of such updates, Information Technology Managers shall verify that the updates have been implemented and are providing the desired results.

**Forms:**

* ITSD102-1 IT SECURITY ASSESSMENT CHECKLIST
* ITSD102-2 IT SECURITY PLAN
* ITSD102-3 IT SECURITY PLAN IMPLEMENTATION SCHEDULE

**References:**

1. **ISO 27002:2013 – INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - CODE OF PRACTICE FOR INFORMATION SECURITY CONTROL**

This ISO standard is part of a family of standards designed to provide a comprehensive set of information security controls and practices. For more, see <http://www.iso.org/iso/catalogue_detail.htm?csnumber=54533>.

**B. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION #800-18, REV. 1 – GUIDE FOR DEVELOPING SECURITY PLANS FOR INFORMATION TECHNOLOGY SYSTEMS (FEB., 2006)**

See <http://csrc.nist.gov/> for details on NIST publications.

**Additional Resources:**

1. van der Walt, Charl, Introduction To Security Policies, Part One: An Overview of Policies, Symantec Corp. (created Aug., 2001; revised Nov., 2001). <http://www.symantec.com/connect/articles/introduction-security-policies-part-one-overview-policies>.
2. Rutgers Office of Information Technology, Developing a Security Plan, <http://rusecure.rutgers.edu/content/developing-security-plan>.

**Revision History:**

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

[This page intentionally left blank]

**ITSD102-1 IT SECURITY ASSESSMENT CHECKLIST**

|  |  |
| --- | --- |
| **Hardware Risk:** |  |
| Is there redundant hardware to allow work to continue in critical areas in the event of a hardware failure? When was this tested last? |  |
| Does the UPS (uninterruptible power supply) notify someone when it goes into operation? When was it last tested? |  |
| Is there a plan to have hardware replaced at regular intervals? |  |
| **Software Risk:** |  |
| Do you have original disks to reinstall software if the hard drive fails? |  |
| Is all software supported? If software is old or unsupported, what are your plans to replace it? |  |
| Is locally developed software supported by an easy-to-reach developer? |  |
| Do you have provisions to continue operation if central services software is not available? |  |
| **Environmental Risk:** |  |
| Is your equipment located so that it is reasonably free from potential dangers (fire, water leaks, etc.)? |  |
| Do UPSs protect all servers and workstations? |  |
| Is the heating, cooling, and ventilation system (HVAC) keeping your equipment at the appropriate temperature and humidity? |  |
| **Network Failure:** |  |
| Do you have physical and remote access to your network devices? |  |
| Do you have the ability to continue to function in the event of a wide area network failure? |  |

|  |  |
| --- | --- |
| **Security Policy:** |  |
| Does the Company have security policies, standards, and processes? Are they hard copy or electronic? |  |
| Are they readily accessible? |  |
| Do security standards identify all individuals responsible for implementing such standards and what their duties are? |  |
| Do the standards identify steps to be taken if there is a physical and/or information security breach? |  |
| Do the standards identify what physical and/or information are most important to protect? |  |
| Are all employees aware of security processes? |  |
| Are all employees aware of Company IT policies? |  |
| **Department Managers:** |  |
| Is there a background and/or reference check on new employees? |  |
| Are there clearly defined system security procedures for IT system administration? |  |
| Are security-related duties clear to IT personnel? |  |
| Is there an orientation course on good security practices for new employees? |  |
| Do all security related IT duties appear in job descriptions? |  |
| Are IT staff members aware of Company codes of conduct that relate to IT security-related positions? |  |
| Do written procedures exist that explain how to perform all IT security related duties? |  |
| Are IT personnel up to date on training for security related duties? |  |
| Do personnel have sufficient authority to accomplish IT security related duties and policies? |  |
| Are there available and competent personnel to back up IT security related duties in the event the regular IT Security Manager is unavailable? |  |
| Are sufficient funds budgeted to cover IT security? |  |
| Does the Company have a process to address incidents or compromises? |  |
| Do employees sign nondisclosure agreements on the use of confidential material/research material? |  |
| Has funding been provided to recycle old computers and operating systems? |  |
| Does the IT staff know to review the security settings and policies? |  |
| Does the IT staff know how to respond to security breaches? |  |
| Does the IT staff know to use user level accounts when not providing administrative services? |  |
| Are best security practices available? |  |
| Can you ensure that any forms of media containing confidential and sensitive information are sanitized before disposal? |  |
| Are you fully aware of your duties, responsibilities, and resources? |  |
| Have you identified and secured systems that hold critical information or applications? |  |
| Have you identified and secured documents designated as “critical?” |  |
| Is equipment that is being disposed of stripped of data before disposal? |  |
| Is appropriate documentation being completed? |  |
| **IT Management:** |  |
| Does the technical staff know to review the security settings and policies? |  |
| Does the technical staff know how to respond to security breaches? |  |
| Does the technical staff know to use user level accounts when not providing administrative services? |  |
| Can you ensure that any forms of media containing confidential and sensitive information are clean prior to disposal? |  |
| Are you fully aware of your duties, responsibilities, and resources? |  |
| Have you identified and secured systems that hold critical information or applications? |  |
| Have you identified and secured documents designated as “critical?” |  |
| Is equipment that is being disposed of stripped of data before disposal? |  |
| Is appropriate documentation being completed? |  |
| **Department User:** |  |
| Is staff instructed on basic workstation security? |  |
| Are users aware that email attachments should not be opened as a regular practice on PCs? |  |
| Are employees aware of the dangers attachments can bring? |  |
| Does staff have written guidelines for protecting their workstations and storage media files? |  |
| **Accounts and Passwords:** |  |
| Is there a policy for selecting strong passwords? |  |
| Is the Company using software that enforces strong passwords? |  |
| Is the IT Security Manager authorized to check for weak passwords? |  |
| Are passwords changed? How often? |  |
| Is the Company planning to use other forms of authentication other than passwords in the future? |  |
| Does the Company have an account removal process? |  |
| Does the Company have a method for identifying unauthorized users? |  |
| Has Company staff received computer security awareness training? |  |
| Is there a document establishing the identity and number of those having root access to departmental information? |  |
| Is the identity of those having remote access to departmental information known? |  |
| Are there written procedures for forgotten passwords? |  |
| Are there written procedures for closing accounts when an employee terminates employment? |  |
| **Privacy and Confidential Data Storage:** |  |
| Are backup files sent offsite to a physically secure location? |  |
| Are files kept onsite in a secure location? |  |
| **Network and Configuration Security:** |  |
| Does the Company have a network diagram that includes IP addresses, room numbers, and responsible parties? |  |
| Is there an IT auditing standard in place? |  |
| Are end users prevented from downloading and/or installing software? How? |  |
| Are contents of system logs protected from unauthorized access, modification, and/or deletion? Is there a retention standard? |  |
| Is the CD-ROM Autorun feature disabled on all workstations? |  |
| Is password caching disabled on all workstations? |  |
| Have “trusted workstations” (workstations with access to critical information) been identified for critical applications? Have special procedures been setup for these? |  |
| Are the trusted workstations secured if used for other purposes? |  |
| Are trusted workstations SSL, SSH, or VPN enabled? |  |
| Are trusted workstations required to have complex passwords? |  |
| Are workstations used by more than one employee secured? How? |  |
| Are chat clients (ICQ, Yahoo Messenger, IM, etc.) managed (if allowed at departmental workstations) and if so, how are they managed? |  |
| What security precautions are taken for dial-in modems? |  |
| Will any clear-test passwords be embedded in SQL scripts for routine functions such as backup and recovery? If so, how will this data be protected? |  |
| Are ActiveX, JavaScript, and Java disabled in web browsers and email programs for all workstations? |  |
| Is remote control software (for example, PCAnywhere) permitted? If so, where? Explain how it is controlled. |  |
| Is the “Administrator” account, and any equivalent accounts, on all workstations limited to the office technical support person? Is it password protected? |  |
| Do administrators only use an administrative account when doing actual administration? |  |
| Can users tell if files have been changed? (Is data integrity software in use?) |  |
| **Operating System(s):** |  |
| Has the internal firewall been activated? |  |
| Has the remote desktop and remote assistance been turned off? |  |
| **Web Servers:** |  |
| Is the web server set to only accept traffic on port 80? |  |
| Is the web server set to reject attempts to remotely administer it? |  |
| Is the web server set to authenticate certain user traffic? |  |
| Have the sample files, scripts, help and development files been removed? |  |
|  |  |
|  |  |
|  |  |
| **FTP:** |  |
| Are all FTP servers set to authenticate users? |  |
| Is this traffic encrypted/secured? |  |
| Are all FTP directories set to either Read or Write but not to both? |  |
| **Email:** |  |
| Is the email server set to scan mail and attachments for viruses? |  |
| Is the email server set to reject attachments? |  |
| Is the email server set NOT to act as a relay? |  |
| Is web access to email secured? |  |
| Are client connections from outside the subnet secured/encrypted? |  |
| **Network**: |  |
| Does the department have an Internet Use Policy? |  |
| Does the department have a network map/diagram? |  |
| Does the department have an inventory of devices attached to the network? |  |
| Are the room jacks mapped to a switch port? |  |
| Is there a policy as to how network services are accessed by users? |  |
| **File Sharing:** |  |
| Is file sharing permitted and secured on any workstation in the department? If so, how is it secured? |  |
| Is file sharing “unbound” from TCP/IP transport (to prevent access from the Internet) while leaving it bound to NetBEUI for local transport? |  |
|  |  |
|  |  |
|  |  |
| **Disaster Planning:** |  |
| Is there a written contingency plan to perform critical processing in the event that onsite workstations are unavailable? |  |
| Do you have a plan to continue departmental business in the event that the Company’s systems are down for an extended period? |  |
| Do you have a partnership with vendors who can help in an emergency if your equipment is damaged due to disaster? |  |
| Is the contingency plan periodically tested to verify it can be followed to resume critical processing? |  |
| **Backup and Recovery:** |  |
| Are critical files regularly backed up? |  |
| Do you store media off site? |  |
| Is the environment of a selected off-site storage area (temperature, humidity, etc.) within the manufacturer’s recommended range for the backup media? |  |
| Are backup files periodically restored as a test to verify they are usable? |  |
| **Change Management:** |  |
| Are records kept of systems changes? |  |
| Is there a process for communication of systems changes? |  |
| Does the Company have a configuration/asset control plan for all hardware and software products? |  |
| Does the Company have a version control plan for software products? |  |
| Does the Company have network and system diagrams of all system resources? |  |
| Are only trained authorized individuals allowed to install computer equipment and software? |  |
| Are maintenance records kept to indicate what repairs and/or diagnostics were performed and by whom? |  |
| **Patching:** |  |
| Are software patches applied to all workstation software, especially operating system, web browser, word processing, spreadsheet, and database regularly? Checked how often? |  |
| Have you created a plan for upgrades and set aside funding to enable you to keep software up to date? |  |
| **Software Licensing:** |  |
| Is all software licensed to the Company? |  |
| Is documentation available (licenses, purchase orders) if proof is necessary (e.g., a software audit is being conducted)? |  |
| **User Awareness Training:** |  |
| Do you require new employees to read any Company documents? |  |
| Does your staff know what’s expected of them regarding security for the Company? |  |
| Would you consider a security workshop for staff? |  |
| **Network and Host Based Security:** |  |
| Intrusion Detection System (Network Based IDS) |  |
| Does the Company have any way of telling that systems have been or are being compromised? |  |
| Has penetration testing been done for the Company? |  |
| Are any workstations running host-based IDSs? |  |
| Host based firewall? |  |
| Is critical data stored on every server protected from compromise? |  |
| Can you monitor if anyone is accessing critical data? |  |
| Is personal firewall software installed and in use? If so, on how many workstations? What are the settings? |  |
| Do you have enough IT staff to manage individual firewalls on all desktops? Network firewall? |  |
| Are settings password protected? |  |
| How often are logs reviewed? |  |
| Is there central monitoring of settings and logs? |  |
| **Antivirus Software:** |  |
| Are all workstations running the latest version of antivirus software, scanning engine, and the virus signature file? |  |
| Is staff aware that the majority of compromises are due to social engineering and the sharing of information? |  |
| Are the monitors for trusted workstations positioned so that information cannot be viewed by anyone other than the intended viewer? |  |
| Is staff aware that the information they handle may be of value to unintended parties? |  |
| Are there guidelines for handling and storing confidential information and cards for one-time passwords? |  |

**ITSD102-2 IT SECURITY PLAN**

(From NIST Special Publication #800-18, Appendix C)

**A. SYSTEM IDENTIFICATION**

Date:

**System Name/Title**

* Unique Identifier and Name Given to the System

**Responsible Organization**

* List organization responsible for the system

**Information Contact(s)**

* Name of person(s) knowledgeable about, or the owner of, the system.

Name:

Title

Address:

Phone:

**Assignment of Security Responsibility**

* Name of person responsible for security of the system.

Name:

Title

Address:

Phone:

**System Operational Status**

If more than one status is selected, list which part of the system is covered under each status.

* Operational
* Under Development
* Undergoing a major modification

**General Description/Purpose**

* Describe the function or purpose of the system and the information processed.
* Describe the processing flow of the application from system input to system output.
* List user organizations (internal and external) and type of data and processing provided.
* List all applications supported by the general support system. Describe each application’s functions and information processed.

**System Environment**

* Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)
* Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
* Include any security software protecting the system and information.

**System Interconnection/Information Sharing**

* List of interconnected systems and system identifiers (if appropriate).
* If connected to an external system not covered by a security plan, provide a short discussion of any security concerns that need to be considered for protection.
* It is required that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems. A description of these rules must be included with the security plan or discussed in this section.

**Applicable Laws or Regulations Affecting the System**

* List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.

**General Description of Information Sensitivity**

* Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is **High**, **Medium**, or **Low**.
* Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

**B. MANAGEMENT CONTROLS**

**Risk Assessment and Management**

* Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

**Review of Security Controls**

* List any independent security reviews conducted on the system in the last three years.
* Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

**Rules of Behavior**

* A set of rules of behavior in writing must be established for each system. The rules of behavior should be made available to every user prior to receiving access to the system. It is recommended that the rules contain a signature page to acknowledge receipt.
* The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should state the consequences of inconsistent behavior or noncompliance. They should also include appropriate limits on interconnections to other systems.
* Attach the rules of behavior for the system as an appendix and reference the appendix number in this section or insert the rules into this section.

**Planning for Security in the Life Cycle**

Determine which phase(s) of the life cycle the system or parts of the system are in. Describe how security has been handled in the life cycle phase(s) that the system is currently in.

**Initiation Phase**

* Reference the sensitivity assessment which is described in Section 3.7, Sensitivity of Information Handled.

**Development/Acquisition Phase**

* During the system design, were security requirements identified?
* Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
* Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
* Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
* If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

**Implementation Phase**

* Were design reviews and systems tests run prior to placing the system in production? Were the tests documented? Has the system been certified?
* Have security controls been added since development?
* Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?
* Include the date of the certification and accreditation. If the system is not authorized yet, include date when accreditation request will be made.

**Operation/Maintenance Phase**

* The security plan documents the security activities required in this phase.

**Disposal Phase**

* Describe in this section how information is moved to another system, archived, discarded, or destroyed. Discuss controls used to ensure the confidentiality of the information.
* Is sensitive data encrypted?
* How is information cleared and purged from the system?
* Is information or media purged, overwritten, degaussed or destroyed?

**Authorize Processing**

* Provide the date of authorization, name, and title of management official authorizing processing in the system.
* If not authorized, provide the name and title of manager requesting approval to operate and date of request.

**C. OPERATIONAL CONTROLS**

**Personnel Security**

* Have all positions been reviewed for sensitivity level?
* Have individuals received background screenings appropriate for the position to which they are assigned.
* Is user access restricted to the minimum necessary to perform the job?
* Is there a process for requesting, establishing, issuing, and closing user accounts?
* Are critical functions divided among different individuals (separation of duties)?
* What mechanisms are in place for holding users responsible for their actions?
* What are the friendly and unfriendly termination procedures?

**Physical and Environmental Protection**

* Discuss the physical protection for the system. Describe the area where processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.)
* Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, and mobile and portable systems.

**Production, Input/Output Controls**

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, software should be listed. In this section, provide a synopsis of the procedures in place that support the system. Below is a sampling of topics that should be reported in this section.

* User support - Is there a help desk or group that offers advice?
* Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information
* Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media
* Audit trails for receipt of sensitive inputs/outputs
* Procedures for restricting access to output products
* Procedures and controls used for transporting or mailing media or printed output
* Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary)
* External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)
* Audit trails for inventory management
* Media storage vault or library-physical, environmental protection controls/procedures
* Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing)
* Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse
* Procedures for shredding or other destructive measures for hardcopy media when no longer required

**Contingency Planning**

Briefly describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster were to occur. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix.

* Any agreements of backup processing.
* Documented backup procedures in including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup).
* Location of stored backups and generations of backups kept.
* Are tested contingency/disaster recovery plans in place? How often are they tested?
* Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

**Hardware and System Software Maintenance Controls**

* Restriction/controls on those who perform maintenance and repair activities.
* Special procedures for performance of emergency repair and maintenance.
* Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).
* Procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.
* Version control that allows association of system components to the appropriate system version.
* Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.
* Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software.
* Change identification, approval, and documentation procedures.
* Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.
* Are test data “live” data or made-up data?
* Are there organizational policies against illegal use of copyrighted software or shareware?

**Integrity Controls**

* Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
* Is reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
* Is password crackers/checkers used?
* Is integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
* Are intrusion detection tools installed on the system?
* Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
* Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?
* Is message authentication used in the system to ensure that the sender of a message is known and that the message has not been altered during transmission?

**Documentation**

Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security of the system to include backup and contingency activities, as well as descriptions of user and operator procedures.

* List the documentation maintained for the system (vendor documentation of hardware/software, functional requirements, security plan, program manuals, test results documents, standard operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, authorization for processing, verification reviews/site inspections).

**Security Awareness & Training**

* The awareness program for the system (posters, booklets, and trinkets)
* Type and frequency of general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training)
* The procedures for assuring that employees and contractor personnel have been provided adequate training

**Incident Response Capability**

* Are there procedures for reporting incidents handled either by system personnel or externally?
* Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?
* Who receives and responds to alerts/advisories (e.g., vendor patches, exploited vulnerabilities)?
* What preventive measures are in place (i.e., intrusion detection tools, automated audit logs, penetration testing)?

**D. TECHNICAL CONTROLS**

**Identification and Authentication**

* Describe the method of user authentication (password, token, and biometrics).
* If a password system is used, provide the following specific information:
* Allowable character set;
* Password length (minimum, maximum);
* Password aging time frames and enforcement approach;
* Number of generations of expired passwords disallowed for use;
* Procedures for password changes;
* Procedures for handling lost passwords, and
* Procedures for handling password compromise.
* Procedures for training users and the materials covered.
* Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).
* Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.
* Describe any token controls used on this system and how they are implemented.
* Describe the level of enforcement of the access control mechanism (network, operating system, and application).
* Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).
* Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).
* State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.
* Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
* Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).
* Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.
* If digital signatures are used, the technology must conform to FIPS 186*, Digital Signature Standard* and FIPS 180-1, *Secure Hash Standard* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures.

**Logical Access Controls**

* Discuss the controls in place to authorize or restrict the activities of users and system personnel within the system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists (ACLs).
* How are access rights granted? Are privileges granted based on job function?
* Describe the system’s capability to establish an ACL or register.
* Describe how users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
* Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent user from accessing the system or applications outside of normal work hours or on weekends.
* Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
* Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
* Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Dept. of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

**Audit Trails**

* Does the audit trail support accountability by providing a trace of user actions?
* Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
* Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (Type of event, when the event occurred, user id associated with the event, program or command used to initiate the event, etc.)
* Is access to online audit logs strictly enforced?
* Is the confidentiality of audit trail information protected if, for example, it records personal information about users?
* Describe how frequently audit trails are reviewed and whether there are guidelines.
* Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?

**ITSD102-3 IT SECURITY PLAN IMPLEMENTATION SCHEDULE**

Task Completion Date

1. Draft Security Plan
2. Submit Plan for review by other managers
3. Edit Security Plan
4. Finalize Security Plan
5. Submit Plan to Board of Directors
6. Revise as necessary
7. Distribute Security Plan Memo to all personnel
8. Distribute Security Plan to Management Staff
9. Meet with Managers
10. Establish means to accomplish security tasks and activities
11. Establish Security Breach Committee
12. Establish Proactive Security Committee
13. Obtain and install required equipment
14. Implement specific programs
15. Evaluate Security Plan implementation
16. Evaluate Security Program
    * Internal review
    * External audit
17. Modify Security Program and Plan

* Schedule Security Plan update

IT Security Manager: Date:

IT Management: Date:

Security Review Committee: Date:

[This page intentionally left blank]