

SYSTEM SECURITY PLAN

NSF, Inc.

October 2005



Revision Sheet

| Release No. | Date | Revision Description |
|-------------|-----------|----------------------------------|
| Rev. 0 | 10/3/2005 | System Security and Privacy Plan |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |



NSF, Inc. System Security Plan Authorization Memorandum

I have carefully assessed the NSF, Inc. System Security Plan for the FILESERVER. This document has been completed in accordance with the requirements of the NIST System Development Methodology.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.



NAME
Project Leader

DATE

NAME
Operations Division Director

DATE

NAME
Program Area/Sponsor Representative

DATE

NAME
Program Area/Sponsor Director

DATE

NAME
IT Security Officer

DATE

1.0 GENERAL INFORMATION

SYSTEM IDENTIFICATION

System Name/Title

- FILESERVER.

Responsible Organization

- NSF, Inc.

Information Contact(s)

- Name of person knowledgeable about the system as well as responsible for the security of the system.

Name: Bret McHone
Title: Enterprise Administrator
Address: 1234 Robin Hood Lane
Phone: (865) 555-4567
E-mail: bret.mchone@college.com

Name: Johnathon Robinson
Title: Enterprise Administrator
Address: 5656 King Richard Road
Phone: (865) 555-4567
E-mail: johnathon.robinson@college.com



System Operational Status

- Under Development

General Description/Purpose

- Will serve as a secure central storage space for members of the NSF network
 - Customer data, employee data, accounting data, human resource data will be stored and accessed by domain users
- FILESERVER will also server as a domain controller
 - The server will authenticate users and apply any GPO or other restriction for that user account
- FILESERVER will serve as the RADIUS server as well
 - AAA server to provide authentication of remote users

System Description

- FILESERVER will utilize the Microsoft Server 2003, Enterprise Edition operating system
- FILESERVER contains a single Pentium IV, 2.8 Ghz processor
- The system will have 512 MB of RAM and two 40 GB hard drives

- The system connects to the network through a 10/100 Intel NIC
- The machine will be stored in a secure room with other servers in an environment best suited for high-end machines
- FILESERVER will be accessible to authenticated network users, both in-house and remote
 - Accessible remotely via a VPN or dial-up connection
- Anti virus, RADIUS, and a DMZ will help to protect the system from hostile attacks

System Interconnection/Information Sharing

- FILESERVER will be connected to the rest of the NSF network through a switch
- Only authenticated users will be allowed access to the FILESERVER system

General Description of Information Sensitivity

| | Confidentiality | Integrity | Availability |
|------------------------|------------------------|------------------|---------------------|
| Customer Info | HIGH | HIGH | HIGH |
| Employee Info | HIGH | HIGH | MEDIUM |
| Salary Info | HIGH | HIGH | MEDIUM |
| Accounting Info | HIGH | HIGH | HIGH |

Information Groups on the Information System

- Accounting/Data Processing Department
- Human Resources Department
- Production Department
- Information System Department



Consequence of Loss of Confidentiality, Integrity, and Availability for Each Information Group

<This section should state the consequence of loss of confidentiality, integrity and availability for each information group to be collected, created, processed, stored, or disseminated on the system.>

2.0 MANAGEMENT CONTROLS

Risk Assessment and Management

- Risk assessment to be completed November 2005.

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

- Only data relating to NSF, Inc. business should be stored on FILESERVER.
- Any files found on FILESERVER that are personal in nature will result in a write up.
- Any inappropriate material found stored on FILESERVER will result in immediate dismissal.
- Other violations are covered by the NSF, Inc. Acceptable Use Policy.
- Old data no longer relevant to NSF, Inc. should be deleted to make room for new data.
- Disk quotas will be enforced utilizing Active Directory user restriction.

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) the system is currently in.

Initiation Phase

- Reference the sensitivity assessment, which is described in the NIST SP800-18, 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.



3.0 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 in the area where application 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, 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 application software should be listed. In this section, provide a synopsis of the procedures in place that support the operations of the application. 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 and can respond to security incidents in a timely manner? Are there procedures in place documenting how to recognize, handle, and report incidents and/or problems?
- 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 application continues to be processed if the supporting IT systems were unavailable. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix. Include descriptions for the following:

- Any agreements for backup processing
 - Documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)
 - Location of stored backups and generations of backups
- 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?
 - Coverage of backup procedures, e.g., what is being backed up?

Application Software Maintenance Controls

- Was the application software developed in-house or under contract?
- Does the government own the software? Was it received from another agency?
- Is the application software a copyrighted commercial off-the-shelf product or shareware? Has it been properly licensed and enough copies purchased for all systems?
- Is there a formal change control process in place and if so, does it require that all changes to the application software be tested and approved before being put into production?
- Are test data Alive≡ data or made-up data?
- Are all changes to the application software documented?
- Are test results documented?
- How are emergency fixes handled?
- Are there organizational policies against illegal use of copyrighted software, shareware?
- Are periodic audits conducted of users= computers to ensure only legal licensed copies of software are installed?
- What products and procedures are used to protect against illegal use of software?
- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

Data Integrity/Validation 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?
 - Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Are password crackers/checkers used?

- Are 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 application 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 in the application and the support systems(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures.

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

Security Awareness and Training

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

4.0 TECHNICAL CONTROLS

Identification and Authentication

- Describe the major application's authentication control mechanisms.
- Describe the method of user authentication (password, token, and biometrics)
- Provide the following if an additional password system is used in the application:
 - Password length (minimum, maximum)
 - Allowable character set,
 - Password aging time frames and enforcement approach,
 - Number of generations of expired passwords disallowed for use
 - Procedures for password changes (after expiration and forgotten/lost)
 - Procedures for handling password compromise
- Indicate the frequency of password changes, describe how changes are enforced, and identify who changes the passwords (the user, the system, or the system administrator).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user ID that is assigned to a single person).
- Describe the self-protection techniques for the user authentication mechanism (passwords are encrypted, automatically generated, are checked against a dictionary of disallowed passwords, passwords are encrypted while in transmission).
- State the number of invalid access attempts that may occur for a given user id 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 identifiers, and group user identifiers) and any compensating controls.
- Describe any use of digital or electronic signatures and the standards used. Discuss the key management procedures for key generation, distribution, storage, and disposal.

Logical Access Controls

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the application. Describe hardware or software features that are designed to permit only authorized access to or within the application, 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 application's capability to establish an ACL or register.
 - Describe how application 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 users 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.

Public Access Controls

If the public accesses the major application, discuss the additional security controls used to protect the integrity of the application and the confidence of the public in the application. Such controls include segregating information made directly accessible to the public from official agency records. Others might include:

- Some form of identification and authentication
- Access control to limit what the user can read, write, modify, or delete
- Controls to prevent public users from modifying information on the system
- Digital signatures
- CD-ROM for on-line storage of information for distribution
- Put copies of information for public access on a separate system
- Prohibit public to access Alive databases
- Verify that programs and information distributed to the public are virus-free
- Audit trails and user confidentiality
- System and data availability
- Legal considerations

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.)
- Is access to online audit logs strictly enforced?
 - Is the confidentiality of audit trail information protected if, for examples, 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.

