

NSF Inc. Site Security Plan

1. Introduction

The NSF Inc. Site Security Plan's purpose is to outline the specific policies and procedures coinciding with this security roadmap documentation. NSF Inc.'s networks both classified and unclassified will remain under jurisdiction for the lifetime of this organizational statement.

2. Background

The Site Security Plan will be utilized for protecting all networks under direct management by NSF Inc. including, but not limited to, all classified and unclassified segments. The NSF Inc. environment is ever-changing and for this reason all aspects should be implemented within a short term period no greater than one year or budgeted within a long term period no greater than two years.

3. Overview

In the past decade, cyber security threats have grown immensely. NSF Inc.'s response to these malicious threats is to set forth good policy and practice in order to combat potential pitfalls of the digital age. Each domain is to be followed without failure by the departments contained within the organization. Any questions in regard to this document may be directed to the Chief Information Officer of NSF Inc.

4. NSF Inc. Management

NSF Inc's management team is as follows:

Gerald Clevenger	CIO
Johnathon Robinson	Enterprise Administrator Linux Administrator
Bret McHone	Enterprise Administrator Linux Administrator
Robert Koch	Project Manager Anti-virus Administrator
Anita Hatfield	IIS Administrator Anti-virus Administrator
James Hydusik	IIS Administrator WSUS Administrator
Clark McSpadden	WSUS Administrator
Shawn Ward	VPN Administrator

5. Environment

Mission Statement: NSF Inc. strives to provide the best quality staff to solve any and all complex security issues for the private and public sector businesses.

Objectives: Our organization has three main objectives:

1. Provide the best possible solutions to security issues posed by organizations.
2. Eliminate common pitfalls of poor security awareness through educating the public.
3. Train employees with the best standards and certify them through certification processes.

Security Environment:

The NSF Inc. security environment has two major, potential risks - human interaction and internet services. These two components stand to deliver the greatest threats and must be mitigated through security measures and educational awareness.

6. Information Systems

All systems have been accredited and certified by both the IS Department and external accreditation sources. These systems must come under review by our staff no later than 180 days after previous accreditation and certification. Internal accreditation and certification must be signed off on by the acting CIO immediately before implementing the system. These systems include, but are not limited to, desktops, servers, portables, and other electronic devices.

7. Security Monitoring

Security monitoring occurs on many facets at NSF Inc. Snort and ISA Server 2004 monitor all break-in attempts, IM conversations, email transmittals, and web site history logging. Packet sniffers such as Ethereal are used to capture packets to identify malicious scripts and code being executed within the secured networks. It is the job of the site security manager to ensure these are monitored and appropriate actions are delivered.

8. Security Coordination

To have true security coordination the order in which this follows will ensure the ability that all areas can and will be securely covered. Each element in the process assists one another and bring the security factor into a full circle. Those who are responsible for the coordination, procedures and execution of each program will be listed. These personnel are the key managers who make sure that all aspects of each area are following standard operating procedures, guidelines, and perform inspections at random for each aspect.

Physical Security

Site Manager: Shawn M. Ward

Duties Include: Site inspections to ensure all physical security guidelines are being met per standard operating procedures as listed within the company policy. To enforce security measures, counter-terrorism training, laws, and securing any vulnerabilities to the place of business.

Physical Security is the first step in facilitating a true secure nature. This is the first step to exclude any unauthorized outside access to the company. This includes guards, transportation of unclassified and classified material, grounds patrol, surveillance, and structural integrity. Without this none of the other security functions could properly operate due to the possibility of physical espionage, threats, theft, or attacks.

Personnel Security

Site Manager: Shawn M. Ward

Duties Include: Training and evaluations for all personnel whom are hired into the company. Security clearance investigations and intelligence is gathered.

Personnel Security is the second step in locking down the system. These protocols assist primarily to keep tabs on those who are hired and to evaluate prospective personnel. This also entails confidential records management on all personnel including key personnel throughout the facility.

Operational Security

Site Manager: Shawn M. Ward

Duties Include: The evaluation of all operations both ongoing and in the future as well. Assists all decisions in force protection nature to ensure the safe and well being of all personnel. This also includes the ability to re evaluate any decisions deemed to extreme and which will need to be re planned.

Operational Security assist in all operational planning's that are ongoing and ensures that all safety, hazards, confidentiality for movements are kept at a reasonable level as not to ascertain any unnecessary deaths or costs.



Comsec

Site Manager: Shawn M. Ward

Duties Include: Inspections of all TS material, communications equipment, distribution of key material, logging and sending of all classified material above secret.

Communication Security ensures that all procedures for the handling of Top Secret material are followed. All messages are routed through the COM center and distributed from the COM center to those who are cleared for the information. Operational requirements also entail that all TS readers and material is properly distributed as per the companies needs. Inspections and briefing to personnel for all material handled and signed for. To also enforce the laws pertaining to the handling of classified information per guidelines brought forth through the NSA and other national security agencies.

9. Laptops and Other Mobile Devices

Employees are allowed limited access with their issued devices that have been accredited and certified by NSF Inc.'s active site security manager(s). Unauthorized access will be treated as a full attack on our networks and the offending individual will be prosecuted to the fullest extent of the law. If found using the network without authorization, this is also grounds for termination of your employment with NSF Inc.

10. Wireless Information Systems

Wireless Security is administered by the Enterprise Administrators instituting both WEP keys and MAC address filtering. Any approved staff may have wireless access as long as their devices are accredited and certified by NSF Inc's IS staff. Violators of this policy may be terminated and prosecuted.

11. Internet Security

The IS Department has instigated a program to eliminate many common threats from malicious worms and harmful spy ware. On the frontline, we have multiple sniffing and firewall devices protecting the perimeter. These include Linux-based snort IDS detection and Windows-based ISA server 2004. The Enterprise Administrators ensure no illicit activities are taking place on a daily routine schedule. Any incidents must be passed along to the appropriate IRT coordinator immediately along with any pertinent information.

12. Denial of Service/Continuity of Service

All secure systems are protected with external Denial of Service protection at various levels from the routers down to the ISA Server 2004 which uses stateful packet detection. Any suspected DoS attacks will be blocked and prevented from damaging internet services.

13. Malicious Code

Malicious threats are mitigated by a sophisticated server loaded with the most recent version of Symantec Corporate Anti-virus Edition. This server is managed by no less than two staff to ensure proper techniques and change management is occurring. No individuals shall execute diskettes and other data containing materials without proper consent from the CIO or other effective managerial figure. Intentional destruction of data is a federal offense punishable to the fullest extent of the law.

14. Email

Email is the responsibility of the Exchange Administrator and/or the Enterprise Administrator in terms of modifying the access of the email system and/or components associated with it. This will also include enforcing and maintaining the security plan set forth for the email system's security.

NSF Inc. has several simple policies that must be adhered to:

1. All email attachments must be scanned by the Anti-Virus program before opening.
2. Attachments are only to be opened from know contacts.
3. Any unknown email with an attachment is to be deleted immediately.
4. Emails containing ".exe" extensions are NOT to be opened under any circumstances.

Failure to follow these guidelines can and will result in disciplinary action.

15. Incident Response Plan

Please see NSF Inc.'s [Incident Response Plan](#) located along with this document.

16. Data Backup and Restoration

Please see NSF Inc.'s [Data Backup Plan](#) located along with this document.

17. Disaster Recovery Preparation

Please see NSF Inc.'s [Disaster Recovery Plan](#) located along with this document.

18. Risk Management

Please see NSF Inc.'s [Risk Management Plan](#) located along with this document.

19. Plan Change Management

Please see NSF Inc.'s [Change Management Plan](#) located along with this document.

20. Training

In accordance with this document, all staff must attend annual training on cyber security awareness and also all staff must read and sign an agreement stating they've read this plan. Staff must be educated on the dangers of social engineering, potential email and file attachment threats, and all security policies and procedures enforced by NSF Inc.

