GSCJY-18-09

RESOLUTION OF THE
GOVERNMENT SERVICES COMMITTEE
OF THE NAVAJO NATION COUNCIL

21st NAVAJO NATION COUNCL – Third Year, 2009

AN ACTION
Relating to Government Services; Approving Policies and Procedures for the Navajo Nation Department Of Information Technology

BE IT ENACTED;

1. The Navajo Nation herby approves the following policies and procedures for the Navajo Nation Department of Information Technology:

    A. "Official Notification of Acceptable Use Procedures for the Computer Systems, the Internet and Network Security for Navajo Nation Department of Information Technology (NNDIT);" Exhibit A
    B. "Navajo Nation Department of Technology (NNDIT) Antivirus Policy" Exhibit B
    C. "Navajo Nation Department of Technology (NNDIT) Password Policy" Exhibit C.
    D. "Navajo Nation Department of Information Technology (NNDIT) Information Technology Security Policy and Procedures." Exhibit D

2. The Navajo Nation Department of Information Technology policies and procedures approved herein shall become effective immediately and shall remain in effect until amended by resolution of the Government Services Committee

CERTIFICATION

I hereby certify the foregoing resolution was duly considered by the Government Services Committee of the Navajo Nation Council at a duly called meeting in Window Rock, Navajo Nation (Arizona), at which a quorum was present and that the same was passed by a vote of 6 in favor and 0 opposed, this 14th day of July , 2009

Ervin Keeswood Sr, Chairperson
Government Services Committee

Motion:	Amos Johnson
Second:	Charles Damon
Vote:	6 in favor 0 opposing

EXHIBIT A

OFFICIAL NOTIFICATION OF ACCEPTABLE USE PROCEDURES FOR THE COMPUTER SYSTEMS, THE INTERNET AND NETWORK SECURITY FOR NAVAJO NATION DEPARTMENT OF INFORMATION TECHNOLOGY (NNDIT)

THE NAVAJO NATION

DEPARTMENT OF INFORMATION TECHNOLOGY
P.O. BOX 5970 WINDOW ROCK, AZ. 86515
PHONE: (928) 871-6520 FAX: (928) 871-7737

Joe Shirley, Jr.
PRESIDENT

Ben Shelly
VICE PRESIDENT

OFFICIAL NOTIFICATION OF ACCEPTABLE USE PROCEDURES FOR THE COMPUTER SYSTEMS, THE INTERNET AND NETWORK SECURITY FOR NAVAJO NATION DEPARTMENT OF INFORMATION TECHNOLOGY (NNDIT)

INTRODUCTION: Navajo Nation Department of Information Technology (NNDIT) provides resources, communication services and business data services by the acquisition of computer equipment and maintaining access to local, regional, national, and international sources of information. NNDIT permits use of its computer systems and information resources by staff who must maintain respect for the public trust through which they have been provided, in accordance with policy and procedures established by NNDIT. These procedures do not attempt to articulate all required or prescribed behavior by its users. Successful operation of the computer system and network requires that all users conduct themselves in a responsible, decent, ethical and polite manner while using the network. The user is ultimately responsible for his/her actions in accessing network services.

GUIDELINES:

1. Access to the computer systems, information networks, and to the information technology environment within the NNDIT systems is a privilege and must be treated as such by all users of the network and its associated systems.
2. The NNDIT systems will be used solely for the purpose of research, communications, and business-relations and operations.
3. Any system which requires password access or for which the NNDIT requires an account, such as Internet/Network, shall only be used by the authorized user. Account owners are ultimately responsible for all activity under their account and shall abide by this policy.
4. The NNDIT technological resources are limited. All users must exercise prudence in the shared use of this resource. The NNDIT reserves the right to limit use of such resources if there are insufficient funds, accounts, storage, memory, or for other reasons deemed necessary by the system operators and/ or administration, or if an individual user is determined to be acting in an irresponsible or unlawful manner.

5. All communications and information accessible and accessed via the NNDIT systems is and shall remain the property of the NNDIT.
6. Staff use shall be supervised and monitored by system operators and authorized staff and shall be related to the NNDIT administration.
7. Any defects or suspected abuse in system accounting, security, hardware or software, shall be reported to the system operators and NNDIT administration.
8. The NNDIT implements content filters for internet access to monitor and block most unacceptable material. This is a valuable tool, but does NOT guarantee that all unacceptable content is blocked. Staff is responsible for the content that they access and will be held responsible for intentionally seeking/obtaining unacceptable media.

UNACCEPTABLE USE: The NNDIT has the right to take disciplinary action, remove computer(s) and networking privileges, and/or take legal action or report to proper authorities, any activity characterized as unethical, unacceptable or unlawful. Unacceptable use activities constitute, but are not limited to, any activity through which any user:

1. Violates such matters as institutional or third party copyright, license agreements or other contracts. The unauthorized use of and/or copying of software is illegal.
2. Interferes with or disrupts other network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer Trojans, Viruses or Worms, distributing quantities of information that overwhelm the system (chain letters, network games, internet radio etc.) and/or using the network to make unauthorized entry into any other resource accessible via the network.
3. Seeks to gain or gains unauthorized access to information resources, obtains copies of, or modifies files or other data, or gains and communicates passwords belonging to other users.
4. Uses or knowingly allows another to use any computer, computer network, computer system(s), program(s), or software to devise or execute a scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations.
5. Destroys, alters, dismantles, disfigures, prevents rightful access to, or otherwise interferes with the integrity of computer-based information resources, whether on stand alone or networked computers.

6. Invade the privacy of individuals or entities.
7. Uses the network for financial, commercial or political activity or personal or private gain.
8. Installs unauthorized software for use on Navajo Nation (NN) computers.
9. Uses the network to access inappropriate materials.
10. Uses the NNDIT systems to compromise its integrity (hacking software) or the integrity of another system(s) and/or network(s) (DOS) or accesses, modifies, obtains copies of, or alters restricted or confidential records or files.
11. Submits, publishes or displays any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.
12. Uses the NNDIT systems for illegal, harassing, vandalizing, inappropriate, or obscene purposes, or in support of such activities is prohibited. Illegal activities shall be defined as a violation of local, state, and/or federal laws. Harassment is defined as slurs, comments, jokes, innuendos, unwelcome compliments, cartoons, pranks, and/or other verbal conduct relating to an individual which: (a) has the purpose or effect of creating an intimidating, hostile or offensive environment; (b) has the purpose or effect of unreasonably interfering with an individual's work performance; or (c) interferes with business operations. Vandalism is defined as any attempt to harm or destroy the operating system, application software or data. Inappropriate use shall be defined as a violation of the purpose and goal of the network. Obscene activities shall be defined as a violation of generally-accepted social standards in the community for use of a publicly-owned and operated communication device.
13. Uses third party email providers (Yahoo, Gmail, Hotmail) for company use and/or materials exchange such as attachment(s) and/or intellectual property of the NN.

NNDIT RIGHTS AND RESPONSIBILITIES:

1. Monitor all activity on the NNDIT network and/or computer systems.
2. Determine whether specific uses of the network are consistent with acceptable use policy.
3. Remove a user's access to the network at any time it is determined that user is engaged in unauthorized activity or violating this acceptable use policy.

4. Respect the privacy of individual user electronic data. The NNDIT will secure the consent of users before accessing their data, unless required to do so by law, or policies of the NNDIT.
5. Take prudent steps to develop, implement and maintain security procedures to ensure the integrity of individual and district files. However, information on any computer system cannot be guaranteed to be inaccessible by other users.
6. Attempt to provide error free and dependable access to technology resources associated with the NNDIT systems. However, NNDIT cannot be held liable for any information that may be lost, damaged, or unavailable due to technical or other difficulties.
7. Ensure that all staff users complete and sign an agreement to abide by the NNDIT acceptable use policy and administrative regulations. All such agreements will be maintained on file in the administration office.

VIOLATIONS/CONSEQUENCES:

1. Staff

   (a) Staff who violates this policy shall be subject to loss of NNDIT systems access up to and including permanent loss of privileges, and discipline up to and including termination or discharge, in accordance with Navajo Nation Personnel Policies, administrations policies, negotiated agreements and applicable laws, and any other NN Council Legislation.

   (b) Violations of law will be reported to law enforcement officials.

   (c) Disciplinary action may be appealed by administration and/or staffs in accordance with existing NNDIT procedures for suspension or loss of staff privileges.

   This will serve as official notification informing all network/email account users that any violation of the above information will result in disciplinary action which could include suspension and/or termination.

Navajo Nation Department of Information Technology
Technology Acceptable Use Procedures Agreement

NNDIT Acceptable Use Procedures document serves as official notification of acceptable use procedures for computer systems and business network access. Staff wishing to utilize these technologies must agree to do so in a responsible, decent, ethical and polite manner.

Staff will be privileged with access to NNDIT technology equipment and network access functions upon agreement of the following statements and complete signatures.

Name of User: _________________________________
(Staff Name) Please print

Initial _______ I have read, understand and agree to follow the "GUIDELINE POLICIES"

Initial_______ I have read and understand the terms of "UNACCEPTABLE USE"

Initial_______ I have read and understand the "NNDIT RIGHTS AND RESPONSIBILITIES"

Initial_______ I have read the "VIOLATIONS/CONSEQUENCES" section and understand that violations to the acceptable use agreement carry serious consequences including permanent loss of privileges, and discipline action with possible termination.
Re: Staff; violations to the acceptable use agreement carry serious consequences including possible suspension, discharge or termination.

____________________________________ _________________
Staff Signature Date

____________________________________ _________________
Administrators Signature Date

This page is to be read, signed and returned to the administration office. Technology privileges will not be allowed without this agreement on file.

EXHIBIT B

NAVAJO NATION DEPARTMENT OF INFORMATION TECHNOLOGY (NNDIT) ANTIVIRUS POLICY

THE NAVAJO NATION

DEPARTMENT OF INFORMATION TECHNOLOGY
P.O. BOX 5970 WINDOW ROCK, AZ. 86515
PHONE: (928) 871-6520 FAX: (928) 871-7737

Joe Shirley, Jr.
PRESIDENT

Ben Shelly
VICE PRESIDENT

Navajo Nation Department of Information Technology (NNDIT)

Antivirus Policy

All Navajo Nation Department of Information Technology (“NNDIT”) employees are expected to understand the danger that viruses can cause to individual company computers as well as the entire network. All Windows computers (clients and servers) connected to the NNDIT computer network (herein referred to as "the network") or networked resources shall have IT department supported antivirus software correctly installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network. If deemed necessary to prevent the propagation of viruses to other networked devices or detrimental effects to the network, computers infected with viruses or other forms of malicious code (herein collectively referred to as "virus" or "viruses") shall be disconnected from the network until the infection has been identified and removed.

The IT department shall see to it that all Windows computers connected to the network shall have IT department supported antivirus software installed on it. If a Windows computer does not have IT department supported antivirus software installed, it shall be installed according to one of the two following methods:

- If the installation source is a distributed CD-ROM, the antivirus software shall be installed, and a complete scan shall be run before establishing any connection to the network. Upon establishing the initial network connection, the virus definitions shall be updated to the most current version immediately and a new scan shall be run before loading or installing any other software or data.
- If the installation source is a NNDIT server, the computer shall be connected to the network for the sole purpose of installing antivirus software from that server. The installation shall be performed immediately upon establishing the initial network connection and virus updates downloaded and installed, and a full scan shall be run before loading or installing any other software or data.

Under all other circumstances, any Windows computer connected to the network, including servers, shall have IT Department supported antivirus software properly installed, configured, and updated before being connected to the network. IT department will make sure that:

- Virus definitions will be updated at least once daily before retrieving email.
- All files on all hard drives will be scanned daily for viruses.

When an enterprise-wide virus attack is in progress, the IT department shall notify the office computing community via the best available method and all files on all hard drives should be scanned immediately using the newest virus definitions available.

Other operating systems or computing platforms shall have comparable protection, if available. In the event that no antivirus protection is available for a particular operating system or platform, anyone using or accessing these unprotected systems shall apply all prudent security practices to prevent infection, including the application of all security patches as soon as they become available. When antivirus software becomes available for an operating system or platform previously lacking antivirus software, it shall be installed on all applicable devices connected to the network.

Any exceptions to this policy must be explicitly approved by the Chief Information Officer.

The Network Security Administrator reviews all Enterprise Antivirus logs on a weekly basis for servers and desktops. The System Administrator will provide documentation of the weekly review.

JUSTIFICATION AND RATIONALE

Availability, performance, and security of the network represent essential core assets to the daily operation of NNDIT. Viruses and other forms of malicious code (worms, Trojans, backdoors, VBS scripts, mass-mailers, etc.) represent a significant threat to these assets. In order to combat this threat, a comprehensive enterprise security policy must include antivirus provisions to detect, remove, and protect against viral infections. Antiviral procedures should include identification of current and potential viral threats, computers and systems at risk of infection, files at risk of infection, infected computers, and infected files. Infection patterns should be tracked and analyzed to identify chronic internal and external threats.

Many virus infections threaten other computers sharing the infected computer's network. Infected computers must be cleared of viral infections immediately. Files that can be cleaned should have the viral code removed, thus returning them to pre-infected state. Files that cannot be cleaned must be quarantined until such time as they can be replaced with uninfected copies. If all efforts at removing viral infection fail, the computer's hard drive must be formatted and all software reinstalled using clean licensed copies. If an infected computer is deemed capable of infecting or affecting other computers or the network, the infected computer must be disconnected from the network until it is serviced by an IT department representative or designee who will verify that the computer is virus-free.

Antivirus activities must be centrally managed. New viruses represent a continual threat, requiring continual research to plan proactive measures against them. Users must be educated about viral threats and the computing practices required to protect against infection. Whenever a new viral threat appears, the user community must be warned about the new threat. Up-to-date antivirus software must be distributed and its availability advertised to the office community.

ESTABLISHED ANTIVIRAL PROCEDURES

Every year, IT department purchases a site license for AntiVirus (AV) to protect office computers and systems from virus infections. Computers purchased for large-scale rollouts are delivered with AV already installed. Whenever IT department personnel set up a new computer, they ensure that AV is installed before or immediately upon connecting the computer to the network.

The site license permits NNDIT employees to have AV on all Windows computers in the office. AV should be installed before releasing a workstation to an end user. However, if for some reason, an oversight has occurred, the IT department will distribute AV software as follows:

- End users can request AV program installation on office computers by contacting IT department.

Distributed software includes documentation for proper installation, configuration, and use of the software (including instructions for automating file scanning and virus definition updates). Symantec provides free incremental updates of program code and virus definitions via the LiveUpdate utility built into AV. In short, everyone connected with NNDIT has easy access AV updates, and AV documentation.

IT department provides end-user support and forwards virus-related service requests (coded with high priority by default) to the appropriate group for rapid response. IT department provides enterprise-level antivirus support and coordination of rapid responses to enterprise-level virus attacks.

REVISION HISTORY

Release No.	Date	Revision Description

REVIEW SCHEDULE

Anti-Virus Definitions - Daily – Automatic
System Scans – Daily – Automatic
Review of Logs – Weekly

OWNER

CIO

DELEGATED OWNER

Network Manager

EXHIBIT C

NAVAJO NATION DEPARTMENT OF INFORMATION TECHNOLOGY (NNDIT) PASSWORD POLICY

THE NAVAJO NATION

DEPARTMENT OF INFORMATION TECHNOLOGY
P.O. BOX 5970 WINDOW ROCK, AZ. 86515
PHONE: (928) 871-6520 FAX: (928) 871-7737

Joe Shirley, Jr.
PRESIDENT

Ben Shelly
VICE PRESIDENT

Navajo Nation Department of Information Technology (NNDIT)

Password Policy

OVERVIEW

Passwords are an important aspect of computer security. Passwords are the line of protection for user accounts. A poorly chosen password may result in the compromise of Navajo Nation Department of Information Technology's (NNDIT) entire network. As such, all NNDIT employees (including but not limited to contractors, vendors, volunteers, interns, and students with access to NNDIT systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

PURPOSE

The purpose of the policy is to establish a standard for creation of strong passwords, the protection of those passwords, the frequency of change and user account lockout.

SCOPE

The scope of the policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any NNDIT facility, has access to the NNDIT network, or stores any non-public Navajo Nation (NN) information.

POLICY

General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed at least every three months.
- Password complexity will be required for all system-level and user-level passwords.
- The minimum password length for all system-level or user-level is eight characters.
- Passwords must be masked and/or hidden from the user during input on all systems.
- All production system-level passwords must meet the system-level password complexity requirements.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months.
- User accounts that have system-level privileges must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication unless encrypted.

- Passwords should be protected verbally, written and electronically. Passwords should not be written down or stored electronically.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of “public”, “private”, and “system” and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMP v2).
- Account lockout is configured for all users on the NNDIT network. The account lockout consists of three failed attempts for duration of 30 minutes.
- All user-level and system-level passwords must conform to the guidelines described below.
- A screen saver password will be configured through a group policy object on all workstation with a timeout set to 30 minutes.

Guidelines

General Password Construction Guidelines

Passwords are used for various purposes at the NN. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (e.g., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is common usage words such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software, etc.
  - The words “NNDIT”, “santafe”, “albuq”, or any derivation.
  - Birthdays and other personal information such as address and phone numbers.
  - Word or numbers patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by digit (e.g., secret1, 1secret)

Note: These passwords are easy to crack.

Common Password Attacks/ Cracks

Password Guessing

Password guessing involves entering common passwords either manually or through programmed scripts. There are many programs available that will cycle through imported lists of users and passwords and these can be large or small depending on the level of knowledge that user has. Password guessing is usually ineffective because it is a laborious process. In the time it takes to guess a password an attack may be detected and the account locked out.

Dictionary Attack

Dictionary attack is a general threat to all passwords. An attacker who obtains some sensitive password-derived data, such as a hashed-password, performs a series of computations using every possible guess for the password. Since passwords are typically small by cryptographic standards, the password can often be determined by brute-force. Depending on the system, the password, and the skills of the attacker, such an attack can be completed in days, hours, or perhaps only a few seconds.

The term dictionary attack initially referred to finding passwords in a specific list, such as an English dictionary. Today, a brute-force approach can compute likely passwords, such as all five-letter combinations, "on-the-fly" instead of using a pre-built list. Since these threats are roughly equivalent, we use the term in the broader sense to include all brute-force attacks.

A password database should always be kept secret to prevent dictionary attack on the data. Obsolete password methods also permit dictionary attack by someone who eavesdrops on the network. Strong methods prevent this.

Brute-force attacks

One of the most common password attacks is the simple brute force dictionary attack. Passwords are stored in the Windows NT SAM and Active Directory after being passed through a one-way hash algorithm. This type of algorithm is not reversible. Therefore, the only way to tell if you have the right password is to run it through the same one-way hash algorithm and compare the results. Dictionary attacks run entire dictionaries through the encryption process, looking for matches. They are a simplistic, yet very effective, approach to finding out who's used common words like "password" or "guest" as their account passwords.

Social-Engineering Attacks

These attacks depend on smooth talking: an attacker uses a mix of persuasive skills ("I can't secure this system without your password", claims of authority, and misdirection ("I'm calling from the IT helpdesk") to fool your users into disclosing their passwords. It's hard to put technical solutions in place to stop these attacks (except, as mentioned, by getting rid of passwords altogether.)

Network Snooping

Network "sniffers" allow attackers to see network traffic in real time. From this traffic, they can pluck out interesting data, including poorly secured passwords. The good news: using strong security protocols like IPSec and Kerberos protects the valuable data by encrypting it, so that the sniffer only records unintelligible information.

Trojan horses

Like the name implies, a Trojan horse is a seemingly innocuous piece of software that the user is tricked into running. Once the software has been run, it can attack the network in a variety of ways in the user's context. One of the many things it can do is watch the user's key strokes and send them to a third party. For example, a Trojan can capture a user's password when she types it in to authenticate to a non-domain resource.

Strong Passwords

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letter (e.g., 0-9, !@#$%^&*()_+~-=\’{}[]:”:<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line, Try to create passwords that can be easily remembered. If the password must be written down it should be placed in a secure area preferably a locked safe. One way to do this is create a password based on song title, affirmation, or other phrase. For example, the phase might be “This May Be One Way To Remember” and the password could be TmB1w2R!” or “Tmb1W>r~” or some other variation.

Note: Do not use either of these examples as passwords!

Password Protection Standards

Do not use the same password for NN accounts as for other non-NN access (e.g., personal ISP accounts, option trading, benefits, etc.). Where possible, don’t use the same password for various NN access needs.

For example, select one password for the Engineering systems and a separate password IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share NN passwords with ANYONE, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential NN information.

Here as a list of “don’ts”:

- Don’t reveal a password over the phone to ANYONE
- Don’t reveal a password in an email message unless encrypted
- Don’t reveal a password to the boss
- Don’t talk about a password in front of other including office staff
- Don’t hint at the format of the password(e.g., “my family name”)
- Don’t reveal a password on questionnaires or security forms
- Don’t share passwords with family members or friends
- Don’t reveal passwords to co-workers at anytime

If someone demands a password, refer them to this document or have them call someone in the IT Department.

Do not use the “Remember Password” feature of application (e.g., Eudora, Outlook, Outlook Express, Netscape Messenger)

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every three months.

Password cracking or guessing may be performed on periodic or random basis by the IT Department or its delegates. If password is guessed of cracked during one of these scans, the user will be required to change it.

Application Development Standards

Application developers must ensure their programs contain the following security precautions.
Applications:

- Should support authentication of individual users, net groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other’s password.
- Should support TACACS+, RADIUS, and/or X.509 with LDAP security retrieval, wherever possible.
- Should not use easy to guess test account (Example: Username: test Password: test)

Use of Password and Passphrases for Remote Access Users

Access to the NNDIT networks via remote access is to be controlled using either one-time password authentication or public/private key system with strong encryption and/or passphrase.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to “unlock” the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of the password and is, therefore, more secure. A passphrase is composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of good passphase: "Jack&JillwentUPtheHILL"

All of the rules above that apply to passwords apply to passphrase.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary actions, up to and including termination.

DEFINITIONS

Terms	Definitions
Application Administration Accounts	Any account that is for the administration of an application (e.g., Oracle database)

REVISION HISTORY

Release No.	Date	Revision Description

REVIEW SCHEDULE

None

OWNER

CIO

DELEGATED OWNER

Network Manager

EXHIBIT D

NAVAJO NATION DEPARTMENT OF INFORMATION TECHNOLOGY (NNDIT) INFORMATION TECHNOLOGY SECURITY POLICY AND PROCEDURE

THE NAVAJO NATION

DEPARTMENT OF INFORMATION TECHNOLOGY
P.O. BOX 5970 WINDOW ROCK, AZ. 86515
PHONE: (928) 871-6520 FAX: (928) 871-7737

Joe Shirley, Jr.
PRESIDENT

Ben Shelly
VICE PRESIDENT

Navajo Nation Department of Information Technology (NNDIT)

Information Technology Security Policy and Procedure

INTRODUCTION

As part of its mission, Navajo Nation Department of Information Technology (NNDIT) acquires, develops, and maintains data and information, computers, computer systems, and networks. These Information Technology (IT) Department resources are intended for business related purposes, including direct and indirect support of the business's instruction, research and service missions; management functions; employee and business life activities; and the free exchange of ideas within the business community and among the business community and the wider local, national, and international communities.

This policy applies to all people who maintain or manage office IT Department resources, their supervisors, and their department managers. It applies to all locations of those resources, whether in the office or from remote locations. This policy is intended to help protect data confidentiality, integrity, availability, accountability, and assurance. Additional policies may govern specific data, computers, computer systems or networks provided or operated by all specific IT Department and subsidiary departments of the business.

IT DEPARTMENT MANAGER(S)

The NNDIT CIO or a designee is responsible for risk assessment, enterprise network intrusion detection, maintaining IT resources contact information, working with IT Department to resolve exposures and reduce potential exposures, and organizing IT security awareness training events.

IT SECURITY MANAGER

The CIO or a designee must appoint an IT security manager. The IT Security Manager is responsible for coordinating security efforts within the company's organizational hierarchy. The IT Department, in coordination with the IT security manager, has the authority and responsibility to direct action as needed to protect IT resources in the company. They have authority to enforce NNDIT IT security policies and direct action related to violations.

To ensure professional management of NNDIT IT resources, the IT Department must ensure that each department follows the NNDIT IT Security Procedures and complies with NNDIT Security Guidelines. Users should not manage NNDIT IT resources. Qualified professional IT consultants may be outsourced to manage or maintain IT Department resources.

GENERAL RULES

All IT security measures must comply with local and/or state and/or federal and/or international laws, NNDIT rules and policies, and the terms of applicable contracts including software licenses. Examples of applicable laws, rules and policies include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the ***Electronics Communications Privacy Act*** and the ***Computer Fraud and Abuse Act***, which prohibit "hacking," "cracking" and similar activities; and the NNDIT ***Acceptable Use Policy***. IT staff with questions as to how the various laws, rules and resolutions may apply to a particular use of NNDIT computing resources should contact the Office of their appropriate legal services for more information.

Requests for exceptions to this policy must be submitted in writing by the department to the IT Security Manager for review. NNDIT will respond to all requests for exceptions in writing.

This policy will be reviewed and updated by IT manager(s) as needed, but at a minimum annually.

UNMANAGED HOSTS

NNDIT recognizes that the IT Department may not manage personally owned IT resources. Unmanaged hosts include computers and other network-connected devices that are not managed by the IT staff. Examples include, but are not limited to personally owned laptops, computers and other devices used in business, at walkups, with wireless. The user of the unmanaged host must comply with the NNDIT ***Acceptable Use Policy*** and all other NNDIT policies.

VENDOR MANAGED HOSTS

Vendors that manage hosts on NNDIT network must be informed of this security policy and sign an Acceptable use Policy and Non Disclosure Agreement to comply with it. The IT Department must maintain contact information for all vendors managing hosts on their network. Requests for exceptions to this policy must be submitted in writing by the department manager to the IT manager(s). NNDIT will respond to all requests for exceptions in writing.

PHYSICAL SECURITY

The IT Department is responsible for the protection of all IT infrastructures, equipment, and hardware located within their organization. The IT Department must document adequate physical security measures for the protection of physical and logical assets, and sensitive applications and data. The IT Department must identify, document, and implement auditable locks where necessary to secure IT resources in their organization. Where possible, IT resources should be aggregated to reduce the cost of physical security and environmental control.

The computer equipment room is locked with a numeric keypad. Only Network/End User IT personnel and the CIO have access to the computer equipment room. Developers and Database personnel do not have access.

Security alarms are present and active after hours and during holidays. If the alarm goes off, the alarm company notifies in the following order: **CIO**, Office Manager, COO.

AUTHENTICATION, AUTHORIZATION, AND AUDIT ABILITY

Department managers, in conjunction with the IT Security Manager, must establish criteria for issuing and revoking accounts.

User and group profiles, primarily through Active Directory, are used to control the level of access to data and information.

User and group profiles, primarily through Active Directory, are used to control the level of access to utilities and databases.

When technically possible, an audit trail must be implemented to track any device connected to the network and the associated users. NNDIT and applicable subsidiary departments must maintain logs according to their Audit Policy.

HOST AND NETWORK SECURITY

In cases where stateful packet inspection is used, network firewalls must be documented and coordinated with Network Services.

NNDIT and applicable subsidiary departments will coordinate the establishment of all external network connections for their department with Network Services. As every external network connection is potentially an entry point for intruders, the IT Department must document all external network connections in their department, including modems.

The American Registry for Internet Numbers (ARIN) is the only standard for NNDIT. NNDIT shall be the only NN program with the authority to apply for and assign numbers on behalf of the NN.

TRAINING AND SECURITY AWARENESS

The IT Department must ensure that all users within their department are aware of, have access to, and comply with the NNDIT ***Acceptable Use Policy***.   They should help to ensure that all people who maintain or manage IT resources within their departments are aware of, have access to, and comply with NNDIT Security Policy.

APPLICATION DEVELOPMENT

The IT Department has the authority and responsibility to ensure a secure development process and deployment of network computer applications intended for use at the NNDIT for processing financial data, employee data, mission critical data, intellectual property or any other data that is sensitive, confidential, or protected by law.

RISK ASSESSMENT

The IT Department will conduct a comprehensive risk analysis of security threats to IT resources for each department at least once every year.

INCIDENT RESPONSE

All NNDIT and subsidiary departments must immediately notify the IT Department of security incidents in their department involving threats to other IT resources. NNDIT and applicable subsidiary IT Department must immediately notify the IT Department of security incidents in their department involving copyright violations or unauthorized privileged access. Law enforcement should be notified of incidents involving threat to property or life, damages in excess of $1,000, or any inappropriate materials examples: hacking, cracking, child pornography. NNDIT and applicable subsidiary IT Department should consult with the NNDIT CIO to determine if law enforcement should be notified. Other incidents should be reported according to the judgment of the IT Department and a Security Incident Report will be filled out and logged.

VIRUS PROTECTION

It is the responsibility of the designated IT staff to ensure up-to-date virus protection on file and print servers; email, web, and any and all servers; and workstations. Please refer to NNDIT ***Anti-Virus Policy*****.**

SOFTWARE INSTALLATIONS

The IT Department has the responsibility to request the removal of software that does not comply with licensing agreements or copyright law, but it is the responsibility of the user to comply with licensing agreements and copyright law as defined in the NNDIT ***Acceptable Use Policy***.

BUSINESS RESUMPTION PLAN

Each department must maintain a business resumption plan. There must be written plans detailing procedures for various disaster scenarios, both natural and man made. To guard against disaster, critical IT resources must be preserved against loss or corruption by appropriate backup procedures.

ENFORCEMENT

Department managers and IT staff who fail to adhere to this policy may be subject to penalties and disciplinary action, both within and outside the organization. Violations will be handled through NNDIT disciplinary procedures applicable to the relevant department or IT employee. NNDIT may temporarily suspend, block or restrict access to IT resources, IT staff, and/or departments independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of NNDIT or other IT resources or to protect NNDIT from liability. NNDIT may also refer suspected violations of applicable law to appropriate law enforcement agencies.

REVISION HISTORY

Release No.	Date	Revision Description

REVIEW SCHEDULE

Yearly

OWNER

CIO

DELEGATED OWNER

Network Manager