

RESOLUTION OF THE
HEALTH, EDUCATION AND HUMAN SERVICES COMMITTEE
23rd NAVAJO NATION COUNCIL - Fourth Year, 2018

AN ACTION

RELATING TO HEALTH, EDUCATION AND HUMAN SERVICES COMMITTEE;
APPROVING THE NAVAJO NATION DEPARTMENT OF DINÉ EDUCATION'S
TECHNOLOGY POLICIES (INFORMATION SECURITY CHARTER POLICY; DATA
CLASSIFICATION POLICY; MANAGEMENT SECURITY POLICY; OPERATIONAL
SECURITY POLICY; TECHNICAL SECURITY POLICY; ACCEPTABLE USE
POLICY) AS APPROVED AND SUBMITTED BY THE NAVAJO NATION BOARD OF
EDUCATION

BE IT ENACTED:

SECTION ONE. AUTHORITY

- A. The Health, Education and Human Services Committee of the Navajo Nation Council has legislative oversight with respect to education on the Navajo Nation, hence the Navajo Department of Diné Education, including the authority to review, recommend or propose adoption of appropriate Plans of Operation and Policies. 2 N.N.C. §§ 400 (C)(1), 401 (C)(1)

SECTION TWO. FINDINGS

- A. The Navajo Nation Board of Education has reviewed and approved by Resolution NNBEFE-423-2018, "Enactment of Technology Policies (Information Security Charter Policy; Data Classification Policy; Management Security Policy; Operational Security Policy; Technical Security Policy; Acceptable Use Policy)". See **Exhibit A** and **Exhibit B**.
- B. Approval and adoption of these policies will bring the Navajo Nation closer to meeting the requirements of the Family Educational Rights Privacy Act allowing the Department of Diné Education access to student-level data with the States of New Mexico, Arizona, Utah and the Bureau of Indian Education.
- C. Approval and adoption of these policies will further the implementation of the Diné School Accountability Plan and the goal of transforming the Department of Diné Education into the level of a state education agency.

- D. These Technology Policies have been reviewed by the Department of Justice and found to be legally sufficient. See **Exhibit C**.
- E. The Health, Education and Human Services Committee of the Navajo Nation Council finds it to be in the best interest of the Navajo Nation to approve the adoption of the these Technology Policies (Information Security Charter Policy; Data Classification Policy; Management Security Policy; Operational Security Policy; Technical Security Policy; Acceptable Use Policy) as found at **Exhibit B**.

SECTION THREE. APPROVAL

The Health, Education and Human Services Committee hereby approves the adoption of the Technology Policies (Information Security Charter Policy; Data Classification Policy; Management Security Policy; Operational Security Policy; Technical Security Policy; Acceptable Use Policy) at **Exhibit B**, as submitted by the Navajo Nation Board of Education for implementation by the Department of Diné Education.

CERTIFICATION

I, hereby, certify that the following resolution was duly considered by the Health, Education and Human Services Committee of the 23rd Navajo Nation Council at a duly called meeting at Tselani/Cottonwood, (Navajo Nation) Arizona, at which a quorum was present and that same was passed by a vote of 3 in favor, 0 opposed, 1 abstained this 09th day of April, 2018.

N - M B, 11

Norman M. Begay, Vice-Chairperson
Health, Education and Human Services Committee
23rd Navajo Nation Council

Motion: Honorable Steven Begay
Second: Honorable Nathaniel Brown



Russell Begaye
President



**DEPARTMENT OF DINÉ EDUCATION
THE NAVAJO NATION**

P.O. Box 670 · Window Rock, Arizona 86515
PHONE (928) 871 – 7475 · FAX (928) 871 – 7474



Jonathan Nez
Vice-President

NNBEFE-423-2018

**RESOLUTION OF THE
NAVAJO NATION BOARD OF EDUCATION**

**Relating to Education; Enactment of Technology Policies (Information Security Charter Policy;
Data Classification Policy; Management Security Policy; Operational Security Policy; Technical
Security Policy; Acceptable Use Policy)**

WHEREAS:

1. The Navajo Nation Board of Education (hereinafter the “Board”) is the education agent in the Executive Branch for the purposes of overseeing the operation of all schools serving the Navajo Nation. 10 N.N.C. § 106 (A). The Board carries out its duties and responsibilities through the Department of Diné Education (hereinafter the “Department”). 10 N.N.C. §106 (G)(3).
2. The Department is the administrative agency within the Navajo Nation with responsibility and authority for implementing and enforcing the educational laws of the Navajo Nation. 2 N.N.C. §1801(B); 10 N.N.C. §107(A). The Department is under the immediate direction of the Navajo Nation Superintendent of Schools, subject to the overall direction of the Board. 10 N.N.C. §107(B).
3. The Health, Education, and Human Services Committee is the oversight committee for the Department of Diné Education and Navajo Nation Board of Education. 2 N.N.C. § 401 (B)(6); 10 N.N.C. § 1(B).
4. The Health, Education and Human Services Committee of the Navajo Nation Council possess subject matter authority “. . . established Navajo Nation policy, promulgate rules and regulations governing... education... of the Navajo Nation government and its tribal organizations...” and “to ensure compliance and implementation of the laws and policies of the Navajo Nation relating to ... education...” 2 N.N.C. §400 (B)(1)-(2).
5. At the moment, the Navajo Nation does not meet the Family Educational Rights Privacy Act (“FERPA”) requirements to receive data on student academic achievement. The Navajo Nation proposes to work towards becoming FERPA compliant, which will allow the Navajo Nation (through the Department of Diné Education, access to student-level data with the state of New Mexico, Arizona, Utah, and the Bureau of Indian Education (“BIE”).
6. The Board finds that the enactment of these technology policies will further the implementation of the Diné School Accountability Plan (“DSAP”) and goal of transforming the Department of Diné Education into a state education agency. These technology policies are attached hereto as “**EXHIBIT**

BOARD OF EDUCATION

*Dr. Pauline M. Begay, President · Marlene Burbank, Vice President · Delores Greyeyes, Secretary
Members: Bennie Begay · Gloria Johns · Patrick D. Lynch · Dr. Bernadette Todacheene
Dr. Tommy Lewis, Jr., Superintendent of Schools*

A.” These specific technology policies are identified as the “Information Security Charter Policy; Data Classification Policy; Management Security Policy; Operational Security Policy; Technical Security Policy; and Acceptable Use Policy.”

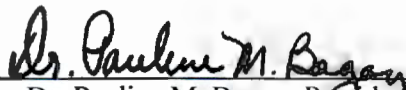
7. The Board also finds that these proposed technology policies will further address findings raised in the Audit Report No. 18-01, which includes implementation of the DSAP.

NOW THEREFORE BE IT RESOLVED THAT:

1. The Navajo Nation Board of Education hereby supports the enactment of technology policies (Information Security Charter Policy; Data Classification Policy; Management Security Policy; Operational Security Policy; Technical Security Policy; Acceptable Use Policy), attached hereto as “EXHIBIT A,” as being in the best interest of the Department of Diné Education and Board.
2. The Board further recommends that the Health, Education, and Human Services Committee of the Navajo Nation Council to enact supporting legislation to establish and enact these policies.
3. The Navajo Nation Board of Education hereby directs and empowers the Superintendent of Schools to take any actions deemed as necessary and proper to carry out the purposes of this resolution.

C E R T I F I C A T I O N

I hereby certify that the foregoing resolution was duly considered by the Board of Education of the Navajo Nation at a duly called meeting at Window Rock, Arizona (Navajo Nation) at which a quorum was present, motion by Bernadette Todacheene and seconded by Bennie Begay and that the same was passed by a vote of 4 in favor; 0 opposed; 0 abstained, this 2nd day of February 2018.



Dr. Pauline M. Begay, President
Navajo Nation Board of Education



DEPARTMENT OF DINÉ EDUCATION TECHNOLOGY POLICIES

Contact:

Brent Nelson, Systems & Programming Manager

E-mail: brentnelson@nndode.org

(928) 871-7718/7452



**DEPARTMENT OF DINÉ EDUCATION
THE NAVAJO NATION**

P.O. Box 670 · Window Rock, Arizona 86515
PHONE (928) 871 – 7475 · FAX (928) 871 – 7474



Russell Begaye
President

Jonathan Nez
Vice-President

February 16, 2018

Honorable Jonathan Hale, Chair
Health, Education and Human Services Committee
23rd Navajo Nation Council
Window Rock, AZ 86515

RE: Enactment of Technology Policies (Information Security Charter Policy; Data Classification Policy; Management Security Policy; Operational Security Policy; Technical Security Policy; Acceptable Use Policy)

Honorable Chairperson Hale:

Attached to this letter is Resolution NNBEFE-423-2018 “Enactment of Technology Policies (Information Security Charter Policy; Data Classification Policy; Management Security Policy; Operational Security Policy; Technical Security Policy; Acceptable Use Policy)” that was approved by the Navajo Nation Board of Education (“Board”) on February 2, 2018.

The Board and Department is requesting your sponsorship of supporting legislation. Upon information and belief, the policies have already obtained any necessary legal reviews and approval by the Navajo Nation Department of Justice. Brent Nelson, is the designated agent and point of contact for this item.

If you have any questions or concerns, please do not hesitate to contact me at (928) 349-5031 or paulabegay17@gmail.com. Thank you.

Respectfully,

Dr. Pauline M. Begay, President
Navajo Nation Board of Education

CC: Dr. Tommy Lewis, Superintendent of Schools/Department of Diné Education
Dr. Timothy Benally, Assistant Superintendent of Schools/Department of Diné Education
Brent Nelson, Systems & Programming Manager /Department of Diné Education

BOARD OF EDUCATION

Dr. Pauline M. Begay, President · Marlene Burbank, Vice President · Delores Greyeyes, Secretary
Members: Bennie Begay · Gloria Johns · Patrick D. Lynch · Dr. Bernadette Todacheene
Dr. Tommy Lewis, Jr., Superintendent of Schools



Russell Begaye
President

**DEPARTMENT OF DINÉ EDUCATION
THE NAVAJO NATION**

P.O. Box 670 · Window Rock, Arizona 86515
PHONE (928) 871 – 7475 · FAX (928) 871 – 7474



Jonathan Nez
Vice-President

NNBEFE-423-2018

**RESOLUTION OF THE
NAVAJO NATION BOARD OF EDUCATION**

**Relating to Education; Enactment of Technology Policies (Information Security Charter Policy;
Data Classification Policy; Management Security Policy; Operational Security Policy; Technical
Security Policy; Acceptable Use Policy)**

WHEREAS:

1. The Navajo Nation Board of Education (hereinafter the “Board”) is the education agent in the Executive Branch for the purposes of overseeing the operation of all schools serving the Navajo Nation. 10 N.N.C. § 106 (A). The Board carries out its duties and responsibilities through the Department of Diné Education (hereinafter the “Department”). 10 N.N.C. §106 (G)(3).
2. The Department is the administrative agency within the Navajo Nation with responsibility and authority for implementing and enforcing the educational laws of the Navajo Nation. 2 N.N.C. §1801(B); 10 N.N.C. §107(A). The Department is under the immediate direction of the Navajo Nation Superintendent of Schools, subject to the overall direction of the Board. 10 N.N.C. §107(B).
3. The Health, Education, and Human Services Committee is the oversight committee for the Department of Diné Education and Navajo Nation Board of Education. 2 N.N.C. § 401 (B)(6); 10 N.N.C. § 1(B).
4. The Health, Education and Human Services Committee of the Navajo Nation Council possess subject matter authority “. . . established Navajo Nation policy, promulgate rules and regulations governing... education... of the Navajo Nation government and its tribal organizations...” and “to ensure compliance and implementation of the laws and policies of the Navajo Nation relating to ... education...” 2 N.N.C. §400 (B)(1)-(2).
5. At the moment, the Navajo Nation does not meet the Family Educational Rights Privacy Act (“FERPA”) requirements to receive data on student academic achievement. The Navajo Nation proposes to work towards becoming FERPA compliant, which will allow the Navajo Nation (through the Department of Diné Education, access to student-level data with the state of New Mexico, Arizona, Utah, and the Bureau of Indian Education (“BIE”).
6. The Board finds that the enactment of these technology policies will further the implementation of the Diné School Accountability Plan (“DSAP”) and goal of transforming the Department of Diné Education into a state education agency. These technology policies are attached hereto as “**EXHIBIT**”

BOARD OF EDUCATION

*Dr. Pauline M. Begay, **President** · Marlene Burbank, **Vice President** · Delores Greyeyes, **Secretary**
Members: Bennie Begay · Gloria Johns · Patrick D. Lynch · Dr. Bernadette Todacheene
Dr. Tommy Lewis, Jr., Superintendent of Schools*

A.” These specific technology policies are identified as the “Information Security Charter Policy; Data Classification Policy; Management Security Policy; Operational Security Policy; Technical Security Policy; and Acceptable Use Policy.”

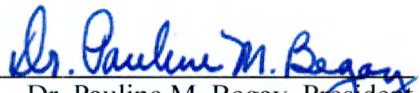
7. The Board also finds that these proposed technology policies will further address findings raised in the Audit Report No. 18-01, which includes implementation of the DSAP.

NOW THEREFORE BE IT RESOLVED THAT:

1. The Navajo Nation Board of Education hereby supports the enactment of technology policies (Information Security Charter Policy; Data Classification Policy; Management Security Policy; Operational Security Policy; Technical Security Policy; Acceptable Use Policy), attached hereto as “EXHIBIT A,” as being in the best interest of the Department of Diné Education and Board.
2. The Board further recommends that the Health, Education, and Human Services Committee of the Navajo Nation Council to enact supporting legislation to establish and enact these policies.
3. The Navajo Nation Board of Education hereby directs and empowers the Superintendent of Schools to take any actions deemed as necessary and proper to carry out the purposes of this resolution.

CERTIFICATION

I hereby certify that the foregoing resolution was duly considered by the Board of Education of the Navajo Nation at a duly called meeting at Window Rock, Arizona (Navajo Nation) at which a quorum was present, motion by Bernadette Todacheene and seconded by Bennie Begay and that the same was passed by a vote of 4 in favor; 0 opposed; 0 abstained, this 2nd day of February 2018.



Dr. Pauline M. Begay, President
Navajo Nation Board of Education

Information Security Charter Policy

Policy Charter





**Title: Information Security Program
Information Security Charter Policy**

Approval

Policy Approved by	Navajo Nation Board of Education Committee
Date Policy Approved	February 2, 2018

Document Change History

Version Number	Release Date	Changes implemented	Sections	Changes implemented by



Title: Information Security Program Information Security Charter Policy

Table of Contents

Navajo Nation Department of Dine' Education	4
Compliance Mandates and Applicable Directives.....	4
Background	5
Management Commitment and Policy Statement	5
Policy Scope.....	6
Policy Documentation	6
Roles and Responsibilities	6
Keywords Definition	10
Policy Revision	10
Policy Exception.....	11
Contact.....	11
Effective Date.....	11
Appendix A	12
Definitions.....	12
Appendix B	16
Policy Waiver.....	16



Navajo Nation Department of Dine Education of Dine Education of Dine Education

Navajo Nation is committed to fostering quality education to Navajo people. Navajo Nation NNDoDE's (hereon represented as NNDoDE) primary focus has been to evaluate academic programs, improve student progress, enhance cultural, academic environment, offer funded support to their communities and to conserve and promote the Navajo culture. The NNDoDE understands the criticality and its responsibility towards protecting the privacy and maintaining security of Personally Identifiable Information, (collected from students, teachers and other clients) and other confidential information as mandated by federal laws, while ensuring the advancement of their community. The NNDoDE has relationships with the following Programs:

- Office of Monitoring, Evaluation and Technical Assistance (OMETA);
- Office of Dine Standards, Curriculum and Assessment (ODSCA);
- AdvanceED (NCAAdvanceED);
- Office of Special Education and Rehabilitation Services (OSERS);
- Office of Navajo Nation Scholarship and Financial Assistance (ONNSFA);
- Office of Youth Development (OYD);
- Office of Dine School Improvement (ODSI);
- Office of Educational Research and Statistics (OERS);
- Johnson O' Malley Program (JOM);
- Office of Navajo Nation Library (NNL); and
- Navajo Head Start (NHS).

Programs have their own Agency sites that are remote office locations.

Compliance Mandates and Applicable Directives

NNDoDE shall adhere to the following compliance standards:

The **Family Educational Rights and Privacy Act (FERPA)** (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student educational records. The law applies to all educational institutions that receive funds under an applicable program of the U.S. Department of Education. FERPA is enforced by the Family Policy Compliance Office, U.S. Department of Education, Washington, D.C.

In addition, the US Education Department of Education has established a Privacy Technical Assistance Center (PTAC) that serves as a data security governance resource and has published a Data Security Checklist that agencies can use to develop their Information Security posture. The



Title: Information Security Program Information Security Charter Policy

checklist refers to ISO 17799 and federal NIST SP 800 standards. Hence we have mapped NNDDoDE security controls to ISO 27002 (upgraded version of ISO 17799) and NIST SP 800-53 (Recommended Security Controls for Federal Information Systems and Organizations) standards.

NIST SP800-53 Standards: National Institute of Standards and Technology (NIST) Special Publications provide extensive guidance and recommendations to help ensure that appropriate security requirements and security controls are applied to all federal information and information systems. NIST guidelines provide an excellent baseline for an information security program.

ISO 27002: The ISO 27002 defines an information security standard published by the International Organization for Standardization (ISO). The standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

Security of Health Records: The Office of Special Education and Rehabilitation Services Program, Head Start Program receive and store health information from its clients for the Vocational & Rehabilitation and Independent Living. Though the program receives limited health information in order to determine benefits it maintains the responsibility of securing the privacy of information.

Background

Information and Information systems are an essential asset and are vitally important to NNDDoDE business operations and long-term viability. The NNDDoDE must ensure that its information assets are protected in a manner that minimizes the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

Management Commitment and Policy Statement

Management is committed to ensuring Confidentiality, Integrity and Availability of its information and information systems. Personnel shall be delegated to give overall strategic direction by approving and mandating the information security principles and operational responsibilities for physical and information security.

This policy establishes the information security program and supporting organizational structure for the NNDDoDE. This policy and related information security policies establish mandatory controls to ensure confidentiality, integrity, availability, reliability, and non-repudiation within the NNDDoDE's infrastructure and its operations. It is the policy of the NNDDoDE that the programs abide by or exceed the requirements outlined in this document and related information security



policies. In addition, to ensure adequate security, NNDoDE programs shall implement additional security policies and procedures as appropriate for their specific operational and risk environment.

Policy Scope

The policy is applicable to all:

- NNDoDE Programs, Program agency sites and program employees;
- NNDoDE owned and managed information systems;
- DoDE Program generated, received, used, stored and transferred data in electronic and paper form;
- Contractors working with data on behalf of the NNDoDE programs; and
- All data regardless of the media on which it resides (including electronic, microfiche, printouts, CD, floppy etc) or the form they may take (text, graphics, video, voice, etc.).

Policy Documentation

The informational security policies are divided into the following primary categories: data classification, management, operational, technical and acceptable use. Together these constitute the information security policies for NNDoDE.

- **NNDoDE P01 - Data Classification Policy** provides the NNDoDE community with a clear understanding of the nature of data classification and proper use of data contained within NNDoDE. This policy outlines the proper use and classification of information assets on NNDoDE systems.
- **NNDoDE P02 - Management Security Policy** focuses on the management of information security systems and the management of risk for a system. They are techniques and concerns that are normally addressed by management.
- **NNDoDE P03 - Operational Security Policy** addresses security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.
- **NNDoDE P04 - Technical Security Policy** focuses on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.
- **NNDoDE P05 - Acceptable Use Policy** outlines the acceptable use of information and information systems within the logical, operational and physical environment.

Roles and Responsibilities



Title: Information Security Program Information Security Charter Policy

The Superintendent or his/her designated committee approves the Information Security Policy or any future revisions. This Information Security Policy assigns executive ownership of and accountability for the NNDODE's Information Security Program to designated personnel within the NEIS Technology staff. The personnel shall be designated as the Systems and Procedures Manager/team. The Systems and Programming Manager must approve Information Security policies.

Management: Senior Officials or assigned designees have planning, budgeting and policy establishment responsibilities within different functional areas. Responsibilities include designating a Systems and Programming Manager, assigning data owners, establishing committees for policy review, approval and establishment and promoting required resources to secure data.

The **Systems and Programming Manager** will appoint a Security team to implement and manage the Information Security Program across NNDODE. The manager is responsible for:

- Creating, maintaining and updating of Information Security policies, standards and guidelines;
- Ensuring consistency of procedures with approved Information Security policies;
- Establishing a Security Awareness Program to ensure that the Information Security Policy and associated policies, standards, guidelines, and procedures are properly communicated and understood across the NNDODE; and
- Heading, investigating and resolving an incident situation by isolating the intrusion and protecting other systems connected to the network until assurance can be made that the problem has been adequately resolved and will not recur.

NEIS Technology staff

The staff is responsible for:

- The operation of a system(s) in support of the program mission;
- Determining, in coordination with the program executive and data owner (Defined in Data Classification Policy), appropriate security controls and identifying resources to implement those controls;
- Developing system rules of behavior for systems under their responsibility;
- Conducting annual reviews and validations of system users' accounts to ensure the continued need for access to a system;
- Enforcing the concept of separation of duties by ensuring that single individuals do not have control of the entirety of a critical process;
- Ensuring that special physical security or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing confidential information (defined in Data classification policy) based on the level of risk;
- Implementing proper system backups, patching security vulnerabilities, and accurately reporting security incidences;



- Utilizing his/her “root” or “administrative” access rights to a computer based on need to know and as needed to perform job functions; and
- Ensuring that the information security posture of the network is maintained during all network maintenance, monitoring activities, installations or upgrades, and throughout day-to-day operations.

Supervisors

Supervisors are responsible for:

- Ensuring compliance with information security policies by all personnel under their direction and providing the personnel, financial and physical resources required to protect information resources appropriately;
- Ensuring that their employees review policies and complete any IT security training that is deployed within the mandated timeframe;
- Notifying the NEIS Technology staff immediately of any unfriendly departure or separation of a NNDoDE employee or contractor if IT staff are not available, then they should contact the appropriate Systems and Programming Manager immediately; and
- Pursuing disciplinary or adverse actions against personnel and contractors who violate the policies and system-specific rules of behavior.

Data Owners

Data Owners are Program Managers and assigned designees who have operational-level responsibility and accountability for the data. Data Owners are responsible for:

- Assigning data classification levels;
- Authorizing data access in systems;
- Defining appropriate requirements for the availability, confidentiality and integrity of the information;
- Establishing the exact nature and extent of authorized access to, and use of information;
- Specifically authorizing individuals for access to information;
- Ensuring that accurate, up-to-date records are kept on access authorities given;
- Regularly checking the continuing validity and proper operation of the protective measures and authorities;
- Reporting occurrences that violate protective measures or threaten to cause an unacceptable risk;
- Ensuring that system owners are aware of the confidentiality of data to be handled and ensuring that data is not processed on a system with security controls that are not adequate with the confidentiality of the data;
- Assigning personnel access to physical areas and physical records within their program;
- Establishing policies, communicating implementation issues to Management and Data Custodians;
- Monitoring compliance with policies;
- Promoting employee education and awareness within their program;



- Communicating suspicious activities to management; and
- Being involved in Incident Response procedures.

Data Custodian: NEIS Technology Staff are typically the data custodians in that they administer, operate, maintain data and computer systems on behalf of the system and data owners. They are responsible for:

- Communicating with data owners regarding data classification level and required security levels;
- Support in identifications of confidential data within systems;
- Implementing secure operational, physical, technical infrastructure, including, but not limited to, granting access privileges to system users, backup and recovery processes, protection standards when data is stored, transferred and disposed of;
- Monitoring data access within systems and applications;
- Evaluating compliance with technical policies;
- Monitoring secure communications; and
- Involvement in Incident Response procedures.

Data User: Data users are personnel who use NNDoDE data as part of their regular business activities. Individuals who are assigned access to confidential data have the responsibility for:

- Protecting the confidentiality, security and integrity of the data;
- Complying with established policies; and
- Communicating any suspicious activities to immediate supervisors and data owners.

Personnel Officers

Personnel officers are responsible for:

- Notifying the NEIS Technology Office within one business day when program personnel are separated from the NNDoDE. If they are not available, the personnel officer should contact the appropriate Systems and Programming Manager.

Users and Employees

The NNDoDE's users and employees are responsible for:

- Complying with the Department of Education's policies, standards, and procedures;
- Being aware they are not acting in an official capacity when using NNDoDE's IT resources for non-department purposes;
- Familiarizing themselves with any special requirements for accessing, protecting, and using data, including compliance requirements, copyright requirements, and procurement-confidentiality data;
- Reporting any suspected or actual computer incidents immediately to the Systems and Programming Manager;



- Seeking guidance from their supervisors when in doubt about implementing this policy document;
- Ensuring that all media containing NNDoDE's Educational data is appropriately marked and labeled to indicate the confidentiality of the data;
- Refraining from loading unapproved software on Department Educational systems or networks;
- Ensuring that sensitive data is not stored on laptop computers or other portable devices unless the data is secured using encryption standards that are commensurate with the confidentiality level of the data;
- Reading, acknowledging, signing, and complying with the Acceptable Use Policy and other Information Security Policies before gaining access to the NNDoDE's systems and networks;
- Implementing specified security safeguards to prevent fraud, waste, or abuse of the systems, networks, and data they are authorized to use;
- Conforming to security policies and procedures that minimize the risk to the NNDoDE's systems, networks, and data from malicious software and intrusions; and
- Agreeing not to disable, remove, install with intent to bypass, or otherwise alter security settings or administrative settings designed to protect NNDoDE's IT resources ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password-protected screen saver before leaving their workstation.

Keywords Definition

The following keywords "SHALL", "SHALL NOT", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED" are utilized within the policies to indicate requirement levels and are to be interpreted as described below:

- **SHALL:** This word, or the terms "REQUIRED" or "MUST," means that the definition is an absolute requirement of the specification.
- **SHALL NOT:** This phrase, or the phrase "MUST NOT," means that the definition is an absolute prohibition of the specification.
- **SHOULD:** This word, or the adjective "RECOMMENDED," means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT:** This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications must be understood and the case carefully weighed before implementing any behavior described with this label.

Policy Revision



Title: Information Security Program Information Security Charter Policy

The Information Security Policies shall be reviewed annually, and when there are significant changes in legal and/or business needs. Annual revision shall be formally approved by Superintendent of Schools and Systems and Programming Manager.

Policy Exception

Any exceptions to this policy will require written authorization and a well-documented justification. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to the Superintendent of Schools.

Contact

For questions and comments regarding the policy contact the Systems and Programming Manager.

Effective Date

The effective date of this policy is the date the policy is approved or as otherwise indicated by approving authority.



Appendix A

Definitions

- **Access**—ability to make use of any information system (IS) resource (Defined in National Institute of Standards and Technology [NIST] Special Publication [SP] 800- 32, Section 9).
- **Access Control**—enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner (Defined in NIST SP 800-27, Appendix B).
- **Accountability**—the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action.
- **Agency sites:** Remote NNDoDE Program office locations.
- **Audit**—a formal (usually independent) review and examination of a project or project activity for assessing compliance with contractual obligations.
- **Audit Trail**—a chronological record of system activities to ensure the reconstruction and examination of the sequence of events and/or changes in an event.
- **Authentication**—verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- **Authorization**—the granting or denying of access rights to a user, program, or Process.
- **Availability**—ensuring timely and reliable access to and use of information.
- **Banner**—display on an information system that sets parameters for system or data use.
- **Best Practices**—the processes, practices, or systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas.
- **Compliance:** Adherence to those policies, procedures, guidelines, laws, regulations and contractual arrangements to which the business process is subject.
- **Confidentiality**—preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Contingency Plan**—a formal document that establishes continuity of operations processes in case of a disaster.
- **Contractor:** Third party that has a valid business agreement with the NNDoDE to perform certain business functions on behalf of the NNDoDE or with valid justification to access NNDoDE data.
- **Critical Assets**—those physical and information assets required for the performance of the site mission.
- **Data**—programs, files or other information stored in, or processed by, a computer system.
- **Database**—a set of related files that is created and managed by a database management system.
- **Department:** NNDoDE
- **Destruction**—the physical alteration of IT media or of IT components such that they can no longer be used for storage or information retrieval.



- **Employee:** A public employee or officer for whom NNDODE is the appointing official.
- **Encryption**—cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.
- **Incident**—a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security.
- **Information**—any communication or representation of knowledge such as facts, data, or opinions in any medium or form; including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.
- **Information Resources**—information and related resources, such as personnel, equipment, funds, and information technology.
- **Information Security**—the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- **Information System**—any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.
- **Label**—marking an item of information to reflect its security classification.
- **Malicious Code**—software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.
- **Management Controls**—the security controls (i.e., safeguards and countermeasures) applied to an information system that focus on the management of risk and the management of the information security system. Actions that are performed primarily to support management decisions with regard to information system security (Defined in NIST SP 800-53, Appendix B).
- **Media**—all materials in which data and/or information may be stored and it may include floppy disks, CD-ROMs, hard drives, software manuals, and papers.
- **Need to Know**—the necessity for access to or knowledge of or possession of specific information required to carry out official duties.
- **Network**—comprises communications media and all components attached thereto whose responsibility is the transfer of information among a collection of IT systems or workstations.
- **Operational Controls**—the security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by people (as opposed to the information system) (Defined in NIST SP 800-53, Appendix B).
- **Patch Management**—the process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization.
- **Portable storage Devices and Portable storage Media include, but not limited to:** USB “sticks” (also known as memory sticks, memory pens, USB flash drives etc), Laptops, notebook computers, personal digital assistants, cellular telephones, Blackberry, iPod’s,



removable drives, External Hard Drives, Zip disks or drives, Cameras and mobile phones/camera phones, MP3/4 or other media players, CDs/DVDs, floppy disks, tapes and other computing and communications devices with network connectivity, storage capability and the capability of periodically operating in different physical locations.

- **Program:** Programs within the NNDoDE.
- **Risk**—the level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring (NIST SP 800-30, Rev A, Appendix E).
- **Risk Assessment**—the process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses (NIST SP 800-30, Rev A).
- **Sanitization**—eliminating sensitive information from an IT system or media associated with an IT to permit the reuse of the IT or media at a lower classification level or to permit the release to unauthorized personnel or personnel without the proper need to know.
- **Scan**—to examine computer coding and programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices (e.g., changes to an executable file, direct writes to specific disk sectors).
- **Security**—the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Defined in 44 U.S.C., SEC. 3542).
- **Security Controls**—the management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, adequately protect the confidentiality, integrity, and availability of the system and its information (Defined in NIST SP 800-53, Appendix B).
- **Security Violation**—the failure to comply with policy and procedures.
- **Separation of Duties**—the practice of dividing roles and responsibilities so that a single individual does not control the entirety of a critical process.
- **Social networking:** blog, wiki, online social network like Twitter, Instagram, Facebook, LinkedIn, Digg or any other form of online publishing.
- **Technical Controls**—the security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system (Defined in NIST SP 800-53, Appendix B).
- **Threat**—any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability.
- **User**—person or process accessing an information system either by direct connections (that is, by way of terminals), or indirect connections.



Title: Information Security Program Information Security Charter Policy

- **Visitors:** Personnel other than agency employees including but not limited to contractors, company representatives, other state entity personnel.
- **Vulnerability**—a flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an organization's operations or assets through a loss of confidentiality, integrity, or availability (Defined in NIST SP 800-53, Appendix B).
- **Vulnerability Assessment**—formal description and evaluation of the vulnerabilities in an information system.



**Title: Information Security Program
Information Security Charter Policy**

Appendix B

Policy Waiver

Date:	
Program Name:	
Program Requester Name:	
Phone Number:	
NNDODE of Dine Educational Policy:	
Justification for noncompliance or deviation:	
Program Director signature and date	
Signature Date	
Timeframe for waiver	
Information Security Officer approval signature and date	

Data Classification Policy

NNDODE-P01





Approval

Policy Approved by	Navajo Nation Board of Education Committee
Date Policy Approved	February 2, 2018

Document Change History

Version Number	Release Date	Changes implemented	Sections	Changes implemented by



Table of Contents

Document Change History.....	2
Policy Purpose.....	4
Scope	4
Compliance	4
Policy Revision	4
Policy Statement - Data Classification Levels	5
Data Classification Matrix	7
Policy Exception.....	9
Contact.....	9



Policy Purpose

The purpose of the policy is to provide the DODE (hereon represented as DoDE) with a clear understanding on confidentiality and sensitivity of data as required by Compliance Laws and business needs. The policy shall outline classification of data that shall determine and define a framework for appropriate use with the Information Security Policies. The policy shall serve as a foundation for the Department's information security policies and shall conform to federal and local laws.

Scope

The policy is applicable to all:

- DODE programs, program agency sites and program employees;
- DODE owned and managed information systems;
- DODE generated, received, used, stored and transferred data in electronic and paper form;
- Contractors working with data on behalf of the DODE; and
- All data regardless of the media on which it resides (including electronic, microfiche, printouts, CD, floppy etc) or the form they may take (text, graphics, video, voice, etc.).

Compliance

All DODE employees are mandated to comply with this policy. Violations shall lead to disciplinary actions including dismissal, expulsion, and/or legal action. Any known violations are to be reported to the Systems and Programming Manager. For further enforcement or clarification on any of the information contained in this policy, please contact the Systems and Programming Manager.

Policy Revision

Policy shall be reviewed and re-approved at least annually, and when there are significant changes to legal, compliance and/or business requirements.



Policy Statement - Data Classification Levels

Information must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed. To provide a basis to determine appropriate security levels, the Department's data (information) is to be classified into one of the following three categories:

I. Confidential

Confidential data is information protected by statutes, regulations, policies or contractual language. It is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure would violate laws and regulations, highly impact DODE, its clients, its employees and its business partners. Decisions about the provision of access to this information must always be cleared through the Data Owner (defined in "Data Ownership" section).

Examples of Confidential Information shall include, but are not limited to:

- Student records and other non-public student data, including student personal information, demographic information, student scores and any other information that directly relates and identifies the student;
- Client personally identifiable information, including full name, date of birth, Social Security numbers, demographic information, drivers license and any other combination of information that directly relates to or identifies the individual;
- Medical records of clients;
- Background check information;
- Personnel and/or payroll records;
- Bank account numbers and other personal financial information;
- System administrator passwords;
- System configurations; and
- System Encryption keys.

Labeling: Records comprising confidential information should be marked as "CONFIDENTIAL." Electronic files with confidential information must have a footer marked as "Confidential Information" or watermarked as "Confidential." Data owners must be identified. Employees must be educated to handle the information in a secure manner.

II. Internal Use Only

Internal Use Only data is intended for restricted use within DODE, based on need-to-know, and in some cases within affiliated organizations such as DODE business partners. This type of information may be widely-distributed within DODE and associated programs, or it could be distributed within the organization without advance permission from the data owner. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions. Classify information as Internal Use Only when the information is intended for use by all employees when conducting DODE business, and including third party contractors who have signed a confidentiality agreement and who have a valid need-to-know. Data not explicitly classified as Confidential or Public will, by default, is classified as Internal Information.



Examples of Internal Information may include, but are not limited to:

- Employment data;
- Personnel directories;
- Internal policies and procedures; and
- Most internal electronic mail messages.

III. Public

Public Information has been specifically approved for public release by a designated authority within the DODE. Examples of Public Information may include material posted to DODE's Internet web pages, newspapers, magazines and brochures. This information may be disclosed outside of the DODE.

Data Owners within Programs should carefully evaluate the appropriate data classification category for their information.

Data in the above mentioned classification levels will require varying administrative, operational and technical security measures appropriate to the degree to which the loss, breach or corruption of the data would impair the functions of DODE or violate federal and local laws.



Data Classification Matrix

	Confidential	Internal Use Only	Public
Access Controls	Must have a business need to know the information. Must have written approval of the data owner.	Generally available to all authorized users on a need to know basis.	Available to the general public. Delete and Change access limited to authorized users.
Personnel Security Controls	Background checks: Combination of Federal, State and Tribal checks.	Reference checks.	Not required.
Training Requirements	Training required.	Providing training would be a good practice.	Not required.
Release to Third Parties	Release is permitted by appropriate policies and procedures. Agreements should be developed requiring non disclosures and complete accountability of data. Information is controlled from creation or acceptance to destruction or return of information.	Intended for use only within the DODE, Information can be shared outside the DODE only if there is a legitimate business need to know, and is approved by the data owner and management, as required.	Available to public.
Audit controls	Access shall be granted by the data owner and audited. Extensive auditing shall be required.	Basic auditing functions: logon/logoff and change in permissions should be audited.	Not required.
Storage controls	Storage shall be in a lockable enclosure. Storage shall be allowed on secure drives only (encryption, strong password). Encrypted storage and backup tape in a secure place or container.	Reasonable precautions shall be taken to prevent access by non-employees. Information can be storage on all DODE drives. Reasonable precautions shall be taken to prevent access by unauthorized personnel	No special precautions Required.



Transfer controls	<p>Protection controls required for electronic transfer. Authorized individuals only allowed for transfer</p> <p>Physical records shall be sealed when transferred.</p> <p>Email is prohibited for transfer of confidential information</p> <p>Confidential data shall be transferred only upon authorization from data owner.</p>	Internal employees are allowed to transfer information.	No special handling Required.
Destruction controls	<p>Electronic data shall be destroyed in a manner that protects confidential information. Destruction of paper should be through shredding or pulping</p> <p>Locked bins must be implemented for hard copy.</p>	Reformatting of electronic information or shredding of records could be adequate methods of disposal.	No special methods.
Replication controls	<p>Copying, printing and other replication of information shall be strictly controlled and extra copies destroyed immediate. Copies of confidential information shall be protected on the same level as original information.</p> <p>Log of replicated information should be maintained.</p>	Replication should be implemented only if required.	No special precautions required.
Physical controls	<p>Information should not be left unattended in an open environment. Sign-off or power-off workstation when not in use or leaving work area.</p>	<p>Password screen-saver to be used when briefly unattended. Sign-off or power-off work stations or terminals when not in use or leaving work.</p>	Sign-off or power-off work stations or terminals when not in use or leaving work.



	Printing of documents when necessary must not be left unattended. Access to areas containing information should be physical restricted. Information must be locked when left in an unattended room. System must not be left unattended at any time unless the information is encrypted or the hardware is secured in a locked file cabinet, room, or safe.		
Labeling	Label all confidential physical records as CONFIDENTIAL. All confidential electronic data should have a confidential label as a watermark or in the footer of the document.	Not required.	Label information as PUBLIC.

Policy Exception

Any exceptions to this policy will require written authorization and a well-documented justification. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to Superintendent of Schools.

Contact

For questions and comments regarding the policy contact the Systems and Programming Manager.



Management Security Policy

NNDODE-P02





Approval

Policy Approved by	Date Policy Approved on
Navajo Nation Board of Education Committee	February 2, 2018

Document Change History

Version Number	Release Date	Changes implemented	Sections	Changes implemented by



Table of Contents

Approval	2
Document Change History	2
Policy Purpose	4
Scope	4
Compliance	4
Policy Revision	4
Policy Statement.....	4
1. Information Security Program	4
2. Systems and Programming Manager.....	Error! Bookmark not defined.
3. Budget and Investment.....	5
4. Systems Life Cycle Process.....	5
5. Security Assessment	5
6. Risk Management	5
7. Information System and Third Party Applications Acquisitions	6
8. Third Party Agreements/Contracts.....	6
Policy Exception.....	7
Contact.....	7



Policy Purpose

The policy establishes directives on the management of security and risks on information and information systems. The policy defines management support, directives and direction towards establishing a security governance program. The policy defines security controls at the management level and includes the following areas:

- Information security program and plan;
- Allocating resources;
- Security budgeting and staffing;
- Information security governance including security roles and responsibilities;
- Risk management programs; and
- Security Assessment and Authorization.

Scope

The policy is applicable to all:

- Department programs, program agency sites and program employees;
- Department owned and managed information systems;
- Program generated, received, used, stored, and transferred data in electronic and paper form;
- Contractors working with data on behalf of the Department programs; and
- Data regardless of the media on which it resides (including electronic, flash drives, microfiche, printouts, CD, floppy etc) or the form they may take (text, graphics, video, voice, etc.).

Compliance

All Department employees are mandated to comply with this policy. Violations shall lead to disciplinary actions including dismissal, expulsion, and/or legal action. Any known violations are to be reported to the Systems and Procedures Manager.

Policy Revision

Policy shall be reviewed annually and when there are significant changes in legal and/or business needs.

Policy Statement

The following paragraphs specify the requirements for information security management policy:

- 1. Information Security Program**



The Department shall develop and disseminate an information security program plan that shall provide a framework of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.

2. Systems and Programming Manager

Information security roles and responsibilities shall be established. A Systems and Programming Manager or personnel delegated with the role shall be designated with the task of developing, implementing, and maintaining a Department-wide information security program and allocating resources for the program.

3. Budget and Investment

Funding requirements for information security technologies and programs shall be explicitly identified within IT operational budgeting plans. Certain costs, such as Department wide training, legal and risk assessments costs, may need to be shared and coordinated with the respective areas within the Department. Systems and Programming Manager shall be charged with the role of establishing methodologies for identifying information security costs for all information systems and networks.

4. Systems Life Cycle Process

A framework shall be established through which the system development life cycle methodology includes information security considerations from inception to the disposal phases of the system through effective management, personnel, operational and technical control mechanisms.

5. Security Assessment

An independent assessor or assessment team shall be employed at least annually to conduct an assessment of the security controls in the administrative, operational and information systems. Planned remedial actions shall be defined to correct deficiencies identified during the assessment of and to reduce or eliminate known vulnerabilities in the system.

6. Risk Management

A thorough analysis of information flow, information networks and systems shall be conducted on a periodic basis to identify and document the threats and vulnerabilities to stored, processed and transmitted information. The analysis shall examine the types of threats – internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource.

The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.



From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined by the Department. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

7. Information System and Third Party Applications Acquisitions

Information System and Third Party application acquisition procedures shall require that vendors/contractors provide documented information describing the security controls available in the system, functional properties of the security controls to be used within the information system, applications, database, other information system components, or information system services in sufficient detail to permit analysis and testing of the controls. Acquisition documents shall mandate that information system components are delivered in a secure, documented configuration, and that the secure configuration is the default configuration for any software reinstalls or upgrades.

8. Third Party Agreements/Contracts

Appropriate safeguards shall be implemented to protect information, information systems and networks from unauthorized access throughout all phases of a contract. Agreements/contracts shall be reviewed to ensure that information security is appropriately addressed in the Agreement/contracting language. Contractors shall be mandated to sign Non Disclosure/Confidentiality Agreements.



Policy Exception

Any exceptions to this policy will require written authorization and a well documented justification. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy shall be addressed to the Systems and Programming Manager.

Contact

For questions and comments regarding the policy contact the Systems and Programming Manager.

Operational Security Policy

NNDODE-P03





Approval:

Policy Approved by	Date Policy Approved on
Navajo Nation Board of Education Committee	February 2, 2018

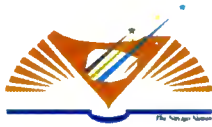
Document Change History

Version Number	Release Date	Changes implemented	Sections	Changes implemented by



Table of Contents

Document Change History	2
Policy Purpose.....	4
Scope	4
Compliance	4
Policy Revision	4
Policy Statement.....	4
1. Personnel Security	5
2. Software Use.....	6
3. Media Control.....	6
4. Configuration Management and Change Control:	7
5. Physical Access	7
6. Contingency Plan.....	9
7. Information Security Awareness and Training.....	10
8. Incident Response	11
9. Operations Management.....	12
Policy Exception.....	14
Contact.....	14



Policy Purpose

The policy establishes directives for the security requirements necessary for protecting the production environment within Department and program agency sites. The policy defines security controls at the operational level and includes:

- Awareness and Training;
- Configuration Management;
- Contingency Planning;
- Incident Response;
- Media Protection;
- Physical Security;
- Personnel Security;
- Software Use; and
- Operations Management.

Scope

The policy is applicable to all:

- Department Programs, Program agency sites and program employees;
- Department owned and managed information systems;
- Program generated, received, used, stored and transferred data in electronic and paper form;
- Contractors working with data on behalf of the Department programs; and
- data regardless of the media on which it resides (including electronic, flash drives, microfiche, printouts, CD, floppy etc) or the form they may take (text, graphics, video, voice, etc.).

Compliance

All Department employees are mandated to comply with this policy. Violations shall lead to disciplinary actions including dismissal, expulsion, and/or legal action. Any known violations are to be reported to the Systems and Programming Manager.

Policy Revision

For enforcement questions or clarification on any of the information contained in this policy, please contact Systems and Programming Manager. Policy shall be reviewed annually and when there are significant changes in legal and/or business needs.

Policy Statement



The following paragraphs specify the requirements for operational information security policy:

1. **Personnel Security**

Describing job functions

Personnel security should be defined from the beginning of staffing process. Job functions requiring access to confidential information must incorporate security requirements in job descriptions and specify employee responsibilities associated with maintaining compliance with required policies. Roles and responsibilities shall be identified based on separation of duties and least privilege.

Background Investigations

All Departmental employees and contractors with access to confidential information as defined in their job functions require suitable federal, state and tribal background investigations to be completed prior to allowing access. All other employees shall have reference checks conducted at the minimum to help validate and/or access a candidate's qualifications, past performance and appropriateness for a particular position.

Acceptable Use

Employees shall be required to read and acknowledge the *Acceptable Use Policy* that limits personal use of all Department IT resources, which include computers, telecommunications equipment, software, e-mail and Internet provided on the Departmental networks.

Confidentiality Agreement/Non Disclosure Agreement

Employees shall be required to read and sign a confidentiality or non-disclosure agreement restricting employee disclosure and use of confidential data. The agreement shall be documented as a part of the personnel file.

Contractors and vendors shall be required to sign non-disclosure agreements before authorizing them access to Department data. Vendor's agreement must document their access to confidential and internal data based on user access privilege.

Security Education and Awareness Training

New hires should receive initial security education and awareness training before being granted permanent access to Departmental systems and networks or within 30 days of hire. All Departmental users should receive annual (refresher) training in security education and awareness. Additional training should be provided to employees with access to confidential data based on the nature of work environment. A log of training provided should be maintained. Training could also include (but not limited to) periodic notifications through email, posters, memo's, staff meeting discussions, luncheon meetings and brochures.

Personnel Access and Separation

Access to confidential and internal data shall be granted based on Access Control Policy documented in the "Technical Security Policy-NNDoDE-P04."



Disciplinary Action

Disciplinary actions shall be enforced against Departmental employees or contractors who violate the Information Security Policies. The severity of the discipline will be dependent on the nature of the violation.

2. Software Use

All computer software purchased and developed by Department employees or contract personnel on behalf of the Department or licensed for Department use is the property of Department and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

Installed Software

- All software packages that reside on computers and networks within Department must comply with applicable licensing agreements and restrictions and must comply with acquisition of software policies.
- The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it shall be removed from the workstation immediately.
- Employees are prohibited from installing any software, executable, or other file to any agency computing device if that software, executable, or other file that was purchased or downloaded for their personal use. Purchased or downloaded software, executable, or other files include, but are not limited to: SKYPE, music files or software, peer-to-peer software and personal files.

3. Media Control

Media (memory sticks, tapes, drives, disk drives, diskettes, internal and external hard drives, paper, microfilm, floppy and portable devices) used to store confidential data should be secured through proper media labeling, when in storage, transport, and disposal. The Department shall implement physical controls and securely store information system media, paper and electronic, based on the highest security category of the information recorded on the media.

Media Marking

All media on Departmental network containing Departmental data shall be appropriately marked and labeled to indicate the confidentiality level of the data.

Inventory

The agency assets shall be inventoried and all results documented on a recurrent basis as an integral part of component installations. Logs, control numbers, or other tracking mechanisms in addition to appropriate physical protection shall be used for media containing information requiring strict access accountability and/or chain-of-custody verification (including media sent off-site for maintenance).

Media Storage

Media must be labeled as “Confidential” or “Internal Use Only” as appropriate, when they contain such information. Stored media containing confidential data and Internal Use information, after



normal business hours and when office is not occupied shall be physically secured with workspace or areas then within a locked container, office, or suite.

Media Transfer

Media used to transfer confidential information between devices or between individuals must be secured by:

- Transfer between devices: When large volumes of confidential information/data are transferred to another computing device, log of the transfer must be recorded.
- Transfer within Programs. When media is reassigned to another user, media shall be “sanitized” before it is given to new owner to remove residual data. Transfer outside Department: When media containing confidential data is transferred outside Department environment, for example, maintenance of hardware, backup tape transfer, it must be logged, either by physical hand-off or by shipping.

Controls shall be implemented over reproduction of confidential information (paper and electronic). Reproduction of privileged information must be limited to the minimum number of copies consistent with operational requirements and any other pertinent reproduction limitations.

Sanitization and Disposal of Information

Media must be sanitized and data removed prior to disposal. Ensure that sanitization and disposal methods are commensurate with the sensitivity and criticality of Departmental data residing on media. Acceptable methods to dispose data are: Electronic data must be disposed through physical destruction, degaussing, overwriting number of times and zeroing a number of times. Physical records must be redacted and shredded or pulverized.

4. **Configuration Management and Change Control:**

- A baseline configuration for the information systems shall be developed. The baseline configuration should provide information about a particular component’s security configurations.
- The security settings of information technology products shall be configured to the most restrictive mode consistent with operational requirements.
- Changes in configuration of information systems shall be authorized, documented, controlled and monitored.
- All change requests shall be formal and approved by the Navajo Nation, Department of Justice.
- A testing environment separate from production environment shall be implemented for testing purposes prior to deployment.
- Authorized personnel shall follow documented rollout procedures to implement approved changes into the production environment.
- Emergency changes to production environment shall be dual authorized by data owner(s), and other stakeholders.

5. **Physical Access**



Access to areas in which confidential data and internal use information is received, stored and processed must be restricted to only appropriately authorized individuals (individuals assigned to access the data).

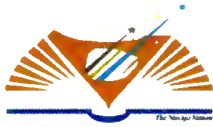
The following physical controls must be implemented in areas where confidential data is received, stored and processed within information systems and in any media format:

- Controlled area: Restricted entry must be implemented for areas that store and process confidential information. All restricted areas must be made to store confidential information in appropriate containers during non-duty hours. Using controlled areas shall eliminate unwanted traffic reducing the opportunity for unauthorized access and/or disclosure or theft of information.
- Implement physical barriers separating restricted and non-restricted areas.
- Designated officials or designee within the Programs shall review and authorize physical access on a need-to-know basis.
- Limit, monitor and log entry points to the area.
- Control access to area through electronic access control, key access or door monitor.
- Maintain employee/visitor logs entering the area. Visitors entering the area shall enter (in ink) in the register: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.
- Secure physical records in locked file cabinets, safes, supply cabinets, open and closed shelving or desk and any other piece of office equipment designed for storing files, documents, papers, or equipment. Key access should be monitored by Program Directors.
- Physical security of systems and other electronic media: Systems that access, store and process confidential information computer operations must be in a secure area with restricted access. DODE program agency sites where confidential data is stored shall receive the highest level of protection that is practical. Security controls such as locking records must be implemented.
- Use surveillance methods to monitor the area.

For Internal Use data designated officials or designee within the Programs shall review and authorize physical access based on need-to-know. Access shall be controlled through key access or door monitors. Records shall be secured during off duty hours in file cabinets, safes and supply cabinets.

Information System physical security

- Critical Information systems such as servers, network devices must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.



- Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. File servers, database, networking equipment containing, transmitting confidential and internal information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
- Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Physical safeguards must include procedures that should:
 - Position workstations to minimize unauthorized viewing of confidential and internal use information;
 - Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to confidential information;
 - Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to confidential information; and
 - Use automatic screen savers with passwords to protect unattended machines.

Visitor Access

- All organization employees shall be issued photo ID badges for access to and within the facility to differentiate employees from visitors;
- Visitors (include all persons other than organization employees or persons under contract to the department) must be required to sign in and sign out every time when at the DODE programs agency premises. Visitors will be issued badges identifying them as visitors for the easy identification.
- The main entrance should be controlled by locating the desk of a responsible employee at the entrance to ensure that only authorized personnel with an official need enter.

6. Contingency Plan

The Department shall establish a Contingency Plan (Business Continuity Plan, Disaster Recovery Plan) to recover from any damage to the information and information system environment within a reasonable period of time. The Department also shall:

- Develop a plan that addresses adverse event and incident preparation, development of an incident response plan, incident reporting, a revised risk assessment, a legal review, and education and awareness training.
- Define procedures for detection, evaluation and to respond to adverse events.
- Define and develop an incident response team for responding to, managing, supporting and participating in incident response activities.
- Develop and regularly maintain an incident response plan to evaluate and determine if an adverse event has become an incident. The plan shall also detail the department incident response team's actions in response to an identified security incident



- Identify alternate processing site that is geographically separated from the primary processing site and fully configure the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.
- Train personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training.

Data backup and Storage

- A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.
- Employees must be educated to store confidential data on shared drives so that they can be backed up. Storage of confidential data on local drives and stand alone devices must be authorized by IT division.
- Backup data must be stored in an off-site location and protected from physical damage.
- Backup data must be afforded the same level of protection as the original data.
- A retrievable, exact copy of confidential information shall be created before movement of equipment.

7. Information Security Awareness and Training

An information security awareness and training program is to be established and maintained to provide continuous education information security to the Department employees, communicate security best practices, and encourage good security practices throughout the organization. The components of the program should include communication processes, training on policies and procedures, and encouraging employees of the Department to become security aware and proactive in preventing incidents.

Security awareness is a key component of the overall information security efforts at NNDoDE. It is important that employees are aware of policies, procedures and how to properly protect the Department's information in its various forms. Employees and others who have access to the Department's information assets need to understand the value of information security, recognize their responsibility for protecting the Department's information and know how to respond when a breach of security occurs.

Information security training is a key element in the overall awareness program. All employees are required to receive training on information security policies and procedures at least annually. Such training will:

- Be made available to all employees annually;
- Be incorporated into the new employee orientation program;
- Include security policies, procedures, risks and other relevant security topics;
- Be updated as frequently as necessary to keep it current with changes in security practices and issues;



- For consultants, contractors and other non-employee users, basic information security requirements and policies are to be communicated to them when they are given access to the Department's systems.

Navajo Education Information Systems technology personnel are responsible for developing and providing the awareness program and training. Other appropriate departments may be selected to assist in delivering the training.

Ongoing communication and other processes are to be used and developed to further educate employees and maintain employees' awareness of security policies, procedures and issues.

8. Incident Response

A Computer Security Incident Response Team (CSIRT) will be established to respond to and manage computer security incidents involving the Department's computer systems, networks or data resources. The CSIRT will define and implement a computer security incident response process to manage incidents when they do occur. CSIRT may also define and direct implementation of proactive measures to mitigate potential incidents.

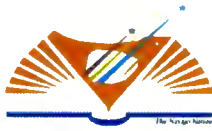
The objectives of the CSIRT and the related process are to:

1. Investigate actual or suspected computer security incidents and intrusion attempts, and report their findings to appropriate management in a timely manner;
2. Ensure that the incident is contained and eradicated, the systems and data are recovered, and the appropriate personnel are informed;
3. Ensure documentation and digital evidence is collected, preserved and protected;
4. Report incidents to authorities as required per regulations (HIPPA, FISMA, PCI, CIPA, FERPA, etc.).

The CSIRT membership will consist of Systems and Programming Manager, Superintendent of Schools, physical Security Officer, representatives from Navajo Nation Department of Justice, Navajo Nation Department of Human Resources, Marketing/Communications (internal and external), Internal Audit, Department Operations, IT management or others as deemed necessary to provide support for computer security incident responses across the Department. Two types of members will comprise the CSIRT team, core members and support members. Core members represent the CSIRT, providing the direction and primary management of the CSIRT. Support members participate in supportive roles and are brought in as needed.

Under the direction and executive support of the Superintendent of Schools, the Systems and Programming Manager has primary responsibility of ensuring the establishment and implementation of the CSIRT and the related processes.

In the interest of maintaining a strong security posture, it is the responsibility of each and every employee or other system user to report computer security incidents. This allows the Department



to address the incident before it results in financial losses and serious damage to the Department's information assets and safeguarding confidential materials.

- Users shall be responsible to report any suspected security violations to the Incident Response Team as defined in the CSIRT process.
- Department shall be required to notify respective individuals and law enforcements agencies, as applicable by federal, state and tribal laws, when it has been determined that there has been or is reasonably believed to have been a compromise of confidential information through unauthorized disclosure.
- Security weaknesses detected by the CSIRT process must be contained, addressed and resolved within a reasonable time limit based on the severity of the problem.
- Serious incidents (e.g., fraud, malicious viruses, theft, or disclosure of proprietary information) shall be escalated **immediately** to DODE program manager/supervisor at the location.
- The facts and logs related to a suspected security violation must be documented and retained in a secure location that cannot be accessed from the affected network device.
- A summary of security incidents shall be reported to DODE Program Manager, Superintendent of Schools, and Systems and Programming Manager.
- All contact with the media is assigned to Senior Public Information Officer.
- The incident response process must be tested periodically (annually at a minimum.).

9. Operations Management

Information systems operating procedures should be documented, maintained, and made available to authorized users who need them.

Documented procedures should be prepared for system activities associated with information technology processing facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, media handling, computer room and electronic mail handling management. Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes shall be authorized by DODE program managers.

The information system operating procedures should include the following information:

- Processing and handling information;
- Backup – adequate backup for all essential information and software for recovery;
- Scheduling requirements, including system interdependencies, job start / stop completion times;
- System restart and recovery procedures for use in the event of system failure;
- Instructions for handling errors or other exceptions, arising during job execution, including restrictions on use of system utilities; and
- Support contacts and information for unexpected operational or system difficulties.
- Special output and media handling instructions, (i.e. special stationary or management of confidential output including procedures for secure disposal of output from failed jobs)



- Management of audit-trail and system log information.

Operator Logs and Practices

Multi-user production information systems must have computer operator logs which document production application start/stop times, system reboot/restart times, system configuration changes, system errors and corrective actions taken, and confirmation that files and output were handled correctly. The Systems and Programming Manager or specialist designated by the Superintendent of Schools must frequently review the logs from the various production systems. The intent of the reviews is to ensure that operators comply with established procedures and to identify problems in need of remedial action.



Policy Exception

Any exceptions to this policy will require written authorization and a well-documented justification. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy shall be addressed to Systems and Programming Manager.

Contact

For questions and comments regarding the policy contact the Systems and Programming Manager.

Technical Security Policy

NNDODE-P04





Approval:

Policy Approved by:	Navajo Nation Board of Education Committee
Date Policy Approved on:	February 2, 2018

Document Change History:

Version Number	Release Date	Changes implemented	Sections	Changes implemented by



Table of Contents

Document Change History.....	2
Policy Statement.....	4
Scope	4
Compliance	4
Policy Revision	4
Policy Implementation.....	4
1. Access Controls	4
2. Authentication and Authorization.....	5
3. Audit and Accountability	9
4. Patch Management.....	10
5. Virus Protection	11
6. Remote Access Controls:	12
7. Mobile & Portable Computing Controls:	13
8. Network Security	14
9. Transmission Security.....	15
10. Wireless Security Controls	15
Policy Exception.....	16
Contact.....	16



Policy Statement

This policy focuses on the technical security requirements necessary for protecting the production environment in the NNDODE agency sites. The policy defines security controls at the technical level and includes the following areas:

Scope

The policy is applicable to all:

- NNDODE employees locally and at NNDODE program agency sites;
- NNDODE owned and managed information systems;
- Program generated, received, used, stored and transferred data in electronic and paper form;
- Contractors working with data on behalf of NNDODE; and
- Data regardless of the media on which it resides (including electronic, microfiche, printouts, CD, floppy, flash drives, external drives, etc) or the form they may take (text, graphics, video, voice, etc.).

Compliance

All NNDODE employees are mandated to comply with this policy. Violations shall lead to disciplinary actions including dismissal, expulsion, and/or legal action. Any known violations are to be reported to the Systems and Programming Manager.

Policy Revision

For enforcement questions or clarification on any of the information contained in this policy, please contact Systems and Programming Manager. Policy shall be reviewed annually and when there are significant changes in legal and/or business needs.

Policy Implementation

The following paragraphs specify the requirements for the technical information security policy:

1. Access Controls

Logical access to information and computing resources must be controlled based on need-to-know and intended usage. To ensure appropriate levels of access by employees, contractors, vendors and other users, a variety of security measures will be instituted and approved. Mechanisms to control access to information and computing resources include (but are not limited to) the following methods:



2. Authentication and Authorization

Authentication provides a way of identifying a user (i.e., with a unique identifier (userid)). Authorization is the process of enforcing policies and determining what types or qualities of activities, resources or services are permitted for each unique user.

- Access to the NNDODE's computer systems and resources is restricted to authorized personnel and is to be used for management approved purposes only. Access is granted based on job function and business need, according to the principle of least privilege. (The principle of least privilege states that access be granted at the most restrictive level needed to be able to perform one's assigned tasks).
- All userid accounts and data access permissions must be requested and approved by the immediate supervisor and data/system owner. Access requests are to be documented to have an auditable and associated written record of each request and authorization.
- Requests for change in access shall require review of existing access levels by data owners.
- All users must be uniquely identified and properly authenticated to the network, application or computing environment when accessing the computing environment locally or remotely (e.g., Userid).
- Each user will be held responsible for any use of their userid and accountable for transactions processed by their userid, except if the userid has been unknowingly misappropriated.
- Shared, generic, or group userids must not be used without specific, written authorization from Information Security and the relevant NNDODE program manager. The authorization must be based on a valid business reason.
- Userid accounts will be locked after 3 attempts of authentication failures, where such system functionality exists and is cost effective.
- Any employee userid that has remained inactive for 90 days must be disabled.
- Use of guest/anonymous accounts are not allowed. Guest accounts are to be disabled. Unnecessary accounts should be removed, disabled, or otherwise secured.
- IT and information security personnel should be notified when employees or other users are terminated or transferred. User accounts for terminated users are to be disabled or deleted on termination date, unless otherwise directed by manager or Navajo Nation Department of Personnel Management. Access permissions for transferred users are to be reviewed by user's new supervisor, and access rights changed according to new job requirements.
- User accounts shall be reviewed quarterly to identify inactive accounts and verify privileges assigned.



- NNDODE technology staff will ensure that systems can detect and deny unauthorized logon attempts by users. Unauthorized attempts will be logged in accordance with the security audit logging requirements.

Authorizations for Contractors and Third Party associates

- All contractors, vendors, business partners and any third party must have a NNDODE program sponsor to serve as a liaison between the non-employee and NNDODE program. The liaison is held accountable for any usage of the third party userid.
- Access given to contractors, vendors, business partners and any third party must be requested and approved by appropriate management and data/system owners.
- Contractor/Vendor access shall be granted based on least privilege as defined in the contract agreements and NNDODE policies.
- Access shall be monitored.
- Contractor/consultant userids will expire at the end of their contract, or after 3 months if not specified, subject to renewal at the request of the liaison.
- Contractor/consultant userids will be disabled after 90 days of inactivity.

Special Access Privileges

Administration and production support personnel need special privileges on the systems for which they are responsible. Authorization to obtain 'Administrative/ Superuser' rights is granted through the NNDODE's approved access request process and approved by Superintendent of Schools or Systems and Programming Manager and relevant system owner.

Administrators/Superusers should have two separate accounts: one as a regular end-user userid, and one as the Administrator or Root. When the superuser or privileged state is no longer required, the user must exit or log-off the privileged state. Normal work is conducted using the regular end-userid.

- Access to operating system code, services, and commands shall be restricted to individuals such as systems programmers, database administrators, network, and security administrators who require access to perform their daily job responsibilities. Users with special privileges will have their access rights reviewed at least annually by the appropriate authority to ensure access is appropriate.
- User accounts with special privileges will have their activity logged, and the logs are to be reviewed for appropriate use.

Access through External Information Systems



- Access of NNDODE's information and computer systems from external information systems (systems other than NNDODE owned) shall be explicitly authorized.
- The following minimum controls shall be implemented on external information systems prior to initiating access:
 - Antivirus software;
 - Patching and security updates are configured, and up-to-date
 - User Authentication and Password
- Employees are prohibited from downloading any Confidential/Internal Use information on the external information system.
- Access from external connections must use secured connection processes and mechanisms as approved and provided by NNDODE's IT services, such as VPN, two factor authentication or other methods.

Accounts Management

- A central User Identification Management system should be implemented to centralize user account and privilege administration.
- Unique user identification (user ID) and authentication is required for all systems and applications that maintain or access Confidential and/or Internal Information. Employees will be held accountable for all actions performed on the system with their user ID.
- The user must secure his/her authentication control (e.g. password) such that it is known only to that employee and the IT personnel. Sharing of passwords is prohibited.
- User identities will be validated before issuing IDs and other credentials. Procedures shall be established for maintaining and managing system user IDs, including procedures for establishing new user accounts, validating existing user accounts, and terminating former user accounts. Inactive IDs shall be deactivated after a period of no activity.
- Vendor, maintenance and emergency accounts should be enabled when required for a defined timeframe.
- Employees must log off the system when leaving the room and leaving for the day.
- Logon banners must be implemented on all systems to inform all users that NNDODE systems are only for NNDODE business and other approved uses consistent with NNDODE policy, to inform that users their activities may be monitored, and to inform the user that they have no expectation of privacy. Logon banners shall be displayed on computer screens during the authentication process.
- For password-based authentication, NNDODE programs will implement controls on the information system to:
 - Protect passwords from unauthorized disclosure and modification when stored and transmitted;
 - Prohibit passwords from being displayed when entered;



- Enforce password minimum and maximum lifetime restrictions;
 - Prohibit password reuse for a specified number of generations; and
 - Verify employee prior to authorizing password reset.
- **Passwords**

Passwords must be used for all 'userid's that provide access to any NNDODE information system or computer resources. Passwords must be complex, strong and hard to guess, and follow the following structure:

 - **Password Construction**

Complex, strong passwords have the following characteristics:

 - A minimum length of at least 8 characters and as long as 15 characters
 - Must have three of the following four elements:
 - Alpha characters;
 - Upper and lower case characters (e.g., a-z, A-Z);
 - Numeric characters; and
 - Special characters such as @, !, \$ and etc.
 - **General Password Rules**
 - Passwords must be changed at a minimum every 90 days.
 - Passwords must not be sent via email messages or other forms of electronic communiqué unencrypted.
 - Passwords should never be written down or stored on-line.
 - The initial passwords issued by a security administrator must be valid only for the user's first on-line session. At that time, the user must be forced to choose another password before proceeding.
 - Password History - maintain and prevent reuse of the 12 most recent passwords.
- NNDODE technology staff will technically enforce password rules and complexity (i.e., where such functionality is available and cost effective).
- **Shared Accounts:** In certain circumstances, where there is a clear business requirement or system limitation, the use of a shared userID/password for a group of users or a specific job can be used by written approval by Systems and Programming Manager.
 - Additional compensatory controls shall be implemented to ensure accountability is maintained. Monitoring of these accounts shall be a priority and conducted more frequently than other accounts. When required, passwords of multi-user system privileged accounts shall be changed more often than normal user accounts.
 - **Default Accounts:** Default administrator accounts shall be renamed, removed, or disabled. The default passwords for these accounts shall be changed if the account is retained, even if the account is renamed or disabled.
 - **Review of User Access Permissions**



Review and verification of userid access permissions to applications and associated data are to be done at least annually. Review may be done on a valid statistical random sample. The security administrators responsible for administering the userids and permissions are to initiate the reviews and coordinate with the systems/data owners. Business Process Owners (BPO) are to review and verify the userid permissions, and document their review and verification.

- **Previous Logon Notification:** Where technically feasible, the information system shall notify the user, upon successful logon (access), of the date and time of the last logon (access).
- 1. **Unsuccessful login attempts:** The information system shall automatically lock the account/node until released by a NNNODDDE technology team when the maximum number of unsuccessful attempts is exceeded.
- **Session Lock:** If a userid is logged on but is inactive for fifteen (15) minutes, then the user session must automatically invoke time-out (i.e., lock and blank the screen or security screen saver). Once timed-out, the user must be required to re-enter the log-on password in order to resume the session. The user must manually invoke time-out (screen saver) or log-off if he or she leaves their terminal or workstation at any time. In certain limited situations, exceptions to the auto timeout are allowed in support of business operational requirements. Exceptions are to be approved via the exception process.

3. **Audit and Accountability**

Audit logging must be implemented for system access and access to applicable confidential Information. Security audit and logging on information systems such as computers, network devices, routers, firewalls, and applications shall be implemented. Audit logging shall be commensurate with the NNNODDDE's risk assessment findings.

- Security audit features for information system assets shall be enabled and configured to be sufficient to track attempted security breaches.
- Audit strategy should capture the information necessary to identify who is accessing NNNODDDE system assets, access attempts and failures, and violations of security policy.
- Appropriate processes and personnel shall be delegated to review and analyze the logs. Network logs (firewall, boundary router, core router, Intrusion Prevention/Intrusion Detection, web filter, email filter), and anti-virus logs should be reviewed daily. User account logs (Active Directory accounts, application user accounts) must be reviewed weekly.
- Controls shall be implemented to protect audit logs from tampering and available for review. Confidentiality and security of audit information shall be ensured
- Audit logs retention period shall be determined based on the information logged. Typically Audit logs related to network, systems, security and confidential information will be retained for 90 days on-line and archived for at least one (1) year. Reports generated from the logs and proof of review should be kept at least one year.



- Logs should capture information sufficient to satisfy an inquiry to determine:
 - All unsuccessful login and authorization attempts,
 - All changes to logical access control authorities (e.g., rights, permissions),
 - Creation, modification and deletion of objects including files, directories and user accounts,
 - Creation, modification and deletion of user accounts and group accounts,
 - Capture: date of the system event; time of the system event, type of system event initiated, and the user account, system account, service or process responsible for initiating the system event, and
 - Capture modifications to administrator account and administrator group account including: escalation of user account privileges commensurate with administrator-equivalent account and adding or deleting users from the administrator group account.

4. Patch Management

- The computer systems used at NNDODE must be kept current with relevant patches, updates and hotfixes based on risk exposure. It is necessary to maintain current versions of operating systems, network components and critical applications in order to maintain productivity, reduce production downtime, and to minimize risk.
- Routine patch process will be implemented to all NNDODE systems and networks in a manner that ensures maximum protection against security vulnerabilities and minimum impact on NNDODE business operations.
- Where technically feasible, system administrators will use automated tools to create a detailed list of all currently installed software on workstations, servers and other networked devices. Manual process will be conducted on any system or device for which an automated tool is not available.
- Systems and software will be evaluated to verify currency of patch and update levels and an analysis of vulnerabilities will be performed.
- System Administrators, Desktop support personnel and information security staff will monitor for new patch and vulnerability announcements. New patches are to be evaluated for risk level, both from the vendor perspective and to NNDODE's risk perspective. 'Critical' or 'important' rated patches are to be evaluated within 5 business days, and then scheduled for testing and implementation within a reasonable time frame based on the risk exposure, but at least within 30 days. Non-critical patches are to be evaluated and implementation can be scheduled for later during a normal maintenance process. Vendor supplied patch documentation will be reviewed in order to assure compatibility with all system components prior to being applied. Updates and releases from vendors must be monitored and tested prior to deployment.
- Where possible, patches will be successfully tested on non-production systems installed with the majority of critical applications/services prior to being loaded on production systems.
- Third Party updates (Explorer, Adobe) must be reviewed, tested and updated periodically.



- Successful backups of mission critical systems will be verified prior to installation of patches and a mechanism for reverting to the patch levels in effect prior to patching will be identified.
- Patches should be applied during an authorized maintenance window.
- Logs will be maintained to indicate which devices have been patched. System logs help record the status of systems and provide continuity among administrators.
- In the event that a patch cannot be applied due to incompatibility or risk assumption, additional precautions will be implemented and documented in the log.

5. Virus Protection

To protect NNDODE's computer resources and data, appropriate anti-virus and anti-malware (malicious software) software must be implemented on NNDODE's various computers and at appropriate network points. The following must be followed to ensure appropriate protection:

Virus Prevention:

1. Virus protection software must be in place on all servers, desktops and at the mail gateway.
2. Multi-level virus protection software should be in place using at least two industry policy virus protection products. For example, Anti-Virus software on the desktops and servers, and Anti-Virus at the network gateway.
3. All virus scanning software must be kept current and in compliance with Information Technology (IT) standard for anti-virus software and version level. Virus protection software should be updated as soon as an update is available. New virus definitions must be updated automatically on a daily basis, when new updates are identified. Anti-virus on client computers should be configured to check for updates at each login/connection.
4. All desktops and servers must be scanned automatically in real time. A full scan must be scheduled to run at least once a week on all desktops and servers.
5. All software code and files received internally and externally must be tested and checked for viruses, if possible, before introduction to the NNDODE's (production) computer resources.
6. All users should be aware of the processes and procedures for dealing with virus incidents.
7. Information Technology (IT) will provide virus protection software and manage updates for all NNDODE owned network resources.
8. NNDODE employees that connect remotely to the NNDODE (via VPN, secured remote access, etc.) must have updated virus protection software on his/her computer before connecting to the NNDODE network.
9. All non-NNDODE employees, such as contractors, consultants and vendors, must have current, up to date anti-virus protection software on their computers when connecting to the NNDODE network resources. The anti-virus software they have must be equivalent to the NNDODE required policies and level of protection.



10. Virus scan results must be monitored and reviewed on a regular basis. These results should be reported to Information Security on a weekly basis.
11. Information Security and technical support staff must subscribe to and monitor virus alert lists.
12. If available, virus protection should be installed on all PDA's. Anti-Virus clients on PDA's should have at minimum one weekly scheduled virus scan. The anti-virus data files on PDA's should be updated regularly (for example, each time user connects to the Internet or network).
13. All removable media brought in to the agency by employees, contractors, vendors and other support personnel will be scanned before they are used.

Virus Incidents:

1. All virus infections must be logged, and treated as security incidents and reported to Information Security.
2. Tools must be in place to monitor and report virus activity.
3. If a desktop or server should become infected with a virus, a Principle Programmer or the appropriate desktop support person must scan it for viruses and remove any that are found. If the virus caused any damage to the workstation/server, it should be restored to its original state. Afterwards, it should be verified that the virus protection software is functioning (i.e., scanning and receiving its updates).

6. Remote Access Controls:

- Remote access is any access to NNDODE information system by a user communicating through an external, non-NNDODE-controlled network (e.g., the Internet).
- Remote access permission shall be granted only to employees who require such access to meet an approved business need or perform prescribed job responsibilities. Remote access should be requested by employee's supervisor and authorized by Systems and Programming Manager.
- Automated mechanisms shall be employed to facilitate the monitoring and control of remote access methods and remote sessions.
- Authenticated employees shall be restricted to appropriate access through the use of internal technology controls (for example, firewalls and/or router Access Control Lists).
- Secure remote access technology and applications must be used. Strong authentication processes, such as two factor authentication, must be used for remote connections to NNDODE's network and computers. Remote connections must be encrypted. If strong authentication capability is not available for certain approved devices, such as for Personal Digital Assistants (PDAs)/mobile email devices, then the available security features must be activated and used. Such features include device passwords, remote lockout or remote file/configuration delete capability.



- Cryptography shall be implemented to protect the confidentiality and integrity of remote access sessions.
- Remote accesses shall be controlled through a limited number of managed access control points or sessions.
- Employees and contractors with remote access privileges must ensure that systems that are remotely connected to NNODE network, is not connected to any other network at the same time.
- All activity from Remote access systems connections shall be logged locally and archived.
- At no time should any NNODE employee provide their login or authentication credentials to anyone, including family members, or allow another person to use their remote access connection.
- NNODE employees must not remove any sensitive information from NNODE systems without prior approval, must position their computer monitors in such that they cannot be readily viewed by unauthorized persons, and must log off their remote computers to ensure a successful session termination.
- All computers connected remotely to the internal NNODE network must use the most up-to-date anti-virus software and must be protected by a firewall or equivalent software on the client computer when using the Internet.

7. Mobile & Portable Computing Controls:

Highest security controls shall be configured on all NNODE owned portable computing and mobile devices. A standard set of controls, physical, technical and operational, that are required for portable devices shall be defined.

- All portable computing devices, computer media and removable components shall be stored in a secure environment. Devices shall not be left unattended without employing adequate safeguards, such as cable locks, restricted access environments or lockable cabinets.
- Employees, when possible shall implement visual control on portable computing devices while traveling. If visual control cannot be maintained, then necessary safeguards shall be employed to protect the physical device, computer media and removable components.
- Portable media shall be assigned to employees based on role. Portable media shall be provided by NNODE technology staff after authorization by supervisors
- Inventory of all NNODE owned portable devices authorized for work use with the NNODE shall be maintained.
- NNODE owned laptops shall be equipped with anti-virus software.
- Mandatory system configuration settings, encryption and software for NNODE owned devices, as per the system hardening requirement and need to know of the employee



authorized with the device shall be implemented. Device operating systems shall be maintained with appropriate vendor security patches and updates.

- Portable computing devices shall not be equipped with administrator privileges unless authorized. Portable computing devices equipped with administrator capabilities shall be assigned higher levels of security in accordance with the increased risk of an IT security breach or loss of the device.
- All NNDODE owned portable computing devices (including blackberry's and other mobile cellular devices) are required to have a password protection or a PIN & device hardening implemented at the minimum.
- Portable media that frequently access and locally store confidential information should be subject to full disk encryption.
- External media and flash drives that store confidential information should be encrypted.
- Portable computing devices can be equipped with the capability of extended connectivity, beyond that of Ethernet or WiFi only when a functional business requirement of a user or user group provides an overriding need. The NNDODE technology staff shall, during the Access Control evaluation of business functions, determine the applicability of extended access for users and groups.
- Unauthorized software and accessories shall not be used or installed on organization owned and authorized portable computing devices.
- In the event of a lost or stolen device, the employee responsible for the equipment shall notify their immediate supervisor or contract manager.
- Authorized portable computing devices shall not be used on non-NNDODE Information Systems.
- Personally owned portable media is prohibited from accessing, processing and storing confidential and internal use data.
- Personally owned portable media is prohibited from use on NNDODE network without authorization from NNDODE technology staff.
- Portable media to be used by contractors should be authorized by NNDODE technology staff and monitored when in use.
- Loss of assigned portable media should be immediately reported to NNDODE technology staff.

8. Network Security

- Network perimeter protection devices such as firewalls, Intrusion Prevention system shall be implemented that can filter certain types of packets to protect devices on the internal network from being directly affected by malicious attacks.
- Controls implemented shall prevent public access into NNDODE's internal network and network perimeter devices shall deny network traffic by default and allow by exception.



- **Firewall:** All incoming and outgoing connections from NNDODE systems and networks to the Internet, intranets, and extranets should be made through a firewall.
- **Network Security Monitoring:** A security event-monitoring program for all NNDODE systems and networks shall be implemented.

9. **Transmission Security**

Technical security mechanisms must be put in place to guard against unauthorized access to confidential information that is transmitted within and outside the agency over a communications network, including wireless networks. Downloading and uploading confidential, and Internal Information between systems must be strictly controlled. The security controls should include, but not limited to:

- Email encryption when confidential information is transmitted within and outside the agency.
- Protection (password protect/encrypt) of backup data.
- Encryption of portable media.

10. **Wireless Security Controls**

- No wireless network or wireless access point shall be installed without the written approval of the Systems and Programming Manager prior to installation
- Suitable security controls include, but not limited to:
 - Disabling broadcast of SSID;
 - Authentication, and encryption of the wireless connection;
 - Media Access Control (MAC) address restriction; and
 - Physical Security controls for access points.
- Access to systems that hold confidential information via a wireless network is not permitted unless appropriate and adequate measures have been implemented. The controls include, but not limited to: authentication, authorization, encryption, access controls, and logging.



Policy Exception

Any exceptions to this policy will require written authorization and a well documented justification. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to the Superintendent of Schools.

Contact

For questions and comments regarding the policy contact the Systems and Programming Manager.

Acceptable Use Policy

NNDODE P05





**Title: Information Security Program
Acceptable Use Policy
NNDODE-P05**



Approval:

Policy Approved by	Date Policy Approved on
Navajo Nation Board of Education Committee	February 2, 2018

Document Change History

Version Number	Release Date	Changes implemented	Sections	Changes implemented by



Table of Contents

Policy Purpose.....	5
Policy Statement.....	5
1. Internet and Email Policy	5
2. Mail (Physical Paper) Security	6
3. Employee Responsibilities	6
4. Installed Software	7
5. Ownership of Software.....	7
6. Data Transfer/Printing.....	7
7. Facsimile Machines security.....	7
8. Confidential Records Security	8
9. Social Networking Policy.....	8
10. Verbal Communications.....	9
11. Unacceptable Use.....	9
Policy Acknowledgement.....	10
Breach of this policy	10
Further advice and information	10



Policy Purpose

This policy provides direction to employees, contractors and other users for acceptable use of the Department's computing resources. As a part of the overall information security policies, this policy highlights for employees areas of common acceptable use of the computer resources and expectations of employees for proper use and care of the computer systems.

Policy Statement

1. Internet and Email Policy

- Employees are expected to use the Internet and email responsibly and productively. Internet access is limited to job-related activities and authorized Department business only. Limited personal use is allowed so long as it does not interfere with work duties or disrupt the systems performance and integrity, and abides by the policies set forth herein. (*Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role*).
- All Internet and email data that is composed, transmitted and/or received by Department computer systems is considered to belong to the Department and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- The equipment, services and technology used to access the Internet and email are the property of the Navajo Nation and the Navajo Nation reserves the right to monitor and access data that is composed, sent or received through its online connections.
- **No expectation of Privacy:** An employee's rights while using the Internet or email via Navajo Nation, Department of Dine Education (NNDODE) resources does not include the right to privacy. NNDODE reserves the express right to monitor and inspect the activities of the employee while accessing the Internet or email at any time. In addition, all software, files, information, communications, and messages downloaded or sent via the Internet or email using NNDODE resources are the NNDODE's records and property of NNDODE.
- All sites, email and downloads may be monitored, filtered and/or blocked by the Department if they are deemed to be harmful and/or not productive to business.
- The installation of non-authorized and non-Department owned software (as determined by the Department, such as instant messaging technology) is strictly prohibited.
- All files downloaded from the Internet must be scanned with anti-virus software approved by the Department.
- No computer used for Internet access can be running peer-to-peer network services.
- No computer used for Internet access can be connected to another Internet Service Provider other than what is provided by the Department.



- Emails sent via the Department email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.

2. Mail (Physical Paper) Security

- Mail that likely contains confidential information should be opened by addressee or authorized personnel.
- To the extent mail is received in an envelope that is not addressed to a specific person, where it is unclear that it is from the subject of and may contain confidential information, the mail may be opened by unauthorized staff, provided that person opening the envelope reviews the least amount of contents needed to determine to whom the mail is addressed and/or what it contains, at which time the mail shall be delivered to the appropriate person.
- The following controls shall be established when Confidential information is mailed externally:
 - The mailing address of the addressee shall be double-checked before sending the mail.
 - Confidential information must not be visible through the envelope, including any window in the envelope.
 - Sealed envelope or an envelope that may be securely closed must be used and it shall not be provided to unauthorized staff or third persons until properly sealed or closed.

3. Employee Responsibilities

As users of NNDODE technology resources, employees have a shared responsibility with the NNDODE technology staff to maintain the integrity of systems, services, and information so that high quality services can be provided to all employees.

Employee responsibilities include:

- Using the Department's technology resources responsibly and appropriately, consistently with the mission and purpose of the Department, and respecting the rights of other users.
- Respecting privacy and maintaining confidentiality of information.
- Understanding the nature of Confidential, Internal Use and Public Information.
- Complying with federal, state, and tribal regulations regarding access and use of information resources. (e.g. The Family Education Rights and Privacy Act, NIST policies, codes of professional responsibility, etc.).
- Maintaining system accounts (to include files, data and processes associated with those accounts) and PC files, data, and processes, which includes taking appropriate action to backup your PC system.
- Employees should not store confidential data on their local PC system and should store them in shared drives.
- Exercise due diligence in protecting computer you connect to the Department network.



- It is the responsibility of employees to practice "safe computing" by establishing appropriate access restrictions for their accounts, by guarding their passwords, and by changing them regularly. Keep your technology accounts (computer, network) secure.
- To not share privileges with others. Access to technology resources is not transferable to other employees, to family members, or to an outside individual or organization.
- If you suspect unauthorized access, report it to your supervisor or the Systems and Programming Manager.

4. Installed Software

- All software packages that reside on computers and networks within organization must comply with applicable licensing agreements and restrictions and must comply with organization acquisition of software policies.
- The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it will be removed from the computer systems immediately.
- Employees are prohibited from installing any software, executable, or other file to any Department computing device if that software, executable, or other file was purchased or downloaded for their personal use. Purchased or downloaded software, executable, or other files include, but are not limited to: SKYPE, music files or software, peer-to-peer software and personal photos.

5. Ownership of Software

All computer software purchased and developed by Department employees or contract personnel on behalf of organization or licensed for Department use is the property of the organization and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

6. Data Transfer/Printing

- Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.
- Copy/Printing machine equipped with a memory, that allows the reprinting of a document previously copied, upon completion of the copy/print job involving documents containing confidential information shall be deleted prior to leaving the machine.
- In the event a copy/print containing confidential information is unusable (because it is not dark enough, etc.) it shall be destroyed by shredding.

7. Facsimile Machines security

- Trusted staff members must be identified at both the sending and receiving end when transferring confidential data. Fax machines shall be placed in secure areas.



- Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes: notification of the sensitivity of the data and the need for protection, notice to unintended recipients to report the disclosure and confirm destruction of the information.

8. Confidential Records Security

The following controls shall be implemented to secure physical records that contain confidential information within NNDODE programs:

- Paper records that include confidential information must be secured. All incidents that may involve the loss or theft of any such paper records must be reported to Program Director and Systems and Programming Manager. Confidential records must be located and used so as to minimize inadvertent disclosure.
- If the confidential record is in use, but not actively being viewed, it shall be closed, covered or placed in a position to minimize inadvertent disclosure. This is especially important in NNDODE program sites.
- When confidential records are in transit information shall be covered, so that no personal identifiers are visible to minimize exposure.
- When in storage confidential records must be stored where there is controlled access. Information shall not be stored in the open and in hallways where information is accessible by unauthorized individuals. Confidential records shall not be stored in open shelves.
- Confidential records shall be stored out of sight of unauthorized individuals, and shall be locked in a cabinet, room or building when not supervised or in use.
- Provide physical access control for Program offices and Agency sites through the following: Locked file cabinets, desks, closets or offices, Keys, electronic ID swipes, keypad systems where codes are changed on a regular basis.
- Management of physical access must be assigned to designated employees within the Program Offices and Agency sites. Access must be removed immediately when the employee's role changes or if terminated.

9. Social Networking Policy

- Employees need to understand that with the ability to use social networking comes responsibility.
- Before any information generated by or for the Department is made public it must be reviewed by the Senior Public Information Officer and the Management appointed designee to ensure that it does not contain confidential information.
- Clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of the Department shall be explicitly mentioned. Employees



shall be clear and shall write in first person. The writing shall be clear that the employee is speaking for themselves and not on behalf of the Department.

- Information published on social networking sites shall comply with the Department's confidentiality and disclosure of proprietary data policies.
- Social media activities shall not interfere with work commitments.
- The malicious use of online social networks, including derogatory language about any member of the department; demeaning statements about or threats to any third party; incriminating photos or statements depicting hazing, sexual harassment, vandalism, stalking, underage drinking, illegal drug use, or any other inappropriate behavior, will be subject to disciplinary action.
- The Department reserves the right to monitor employee use of social media, monitor, implement controls and block inappropriate web access.
- Sanctions for failure to agree and adhere to this policy will result in actions ranging from reprimand or suspension to dismissal from the Department authorized by the Superintendent or his designee.

10. Verbal Communications

Employees should be aware of their surroundings when discussing confidential information. This includes the use of cellular telephones in public areas. Staff should not discuss confidential information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

11. Unacceptable Use

Unacceptable use of the internal computing resources by employees or other users includes, but is not limited to:

- Access to sites that contain obscene, hateful, pornographic, unlawful, violent or otherwise illegal material;
- Access to all video and audio streaming sites including, but not limited to: Youtube, Vevo, Hulu, Netflix, Crackle, Viewster and other sites hosting video and content that are counterproductive to business operations.
- Downloading, installing and changing desktop backgrounds and screensavers.
- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via NNDODE's email service.
- Using NNDODE computers to perpetrate any form of fraud, and/or software, film or music piracy.
- Stealing, using, or disclosing someone else's password.
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.



- Circumventing or overriding any security mechanism belonging to the NNDODE through IT resources and access provided.
- Sending or posting information that is defamatory to the Department, its products/services, colleagues and/or customers.
- Introducing malicious software onto NNDODE network and/or jeopardizing the security of the organization's electronic communications systems.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of the organization.
- Altering, stealing customer credit card information.

If an employee is unsure about what constituted acceptable internal resource usage, then he/she should ask his/her supervisor and/or the IT manager for further guidance and clarification.

Policy Acknowledgement

No NNDODE employee shall be authorized to use the Department's internal resources until he or she has signed a document indicating that the employee has read and agrees to be bound by the terms of the information security policies. Upon hiring, each new employee will receive a copy of the Information Security policies. Employees should review and acknowledge these policies within 30 days of hire.

Breach of this policy

Any willful and/or deliberate breach of this policy or other information security policies will be viewed as a serious disciplinary offence and may result in actions up to and including termination of employment for employees. Legal actions also may be taken for violations of applicable regulations and laws under which an offender may be prosecuted or be subject to a claim for damage or distress by a data subject.

Further advice and information

For advice on appropriate security measures or other aspects of this policy, contact the Systems and Programming Manager.



Acknowledgement

I have read, understood and shall abide by the policies defined in this document. As NNDODE provides updated policy or procedure information, I accept responsibility for reading and abiding by the changes.

Name (first name last name) _____

Program Name: _____

Signature: _____ **Date:** _____

This Signature Page is to be completed by the employee and given to the Personnel Department who is responsible for keeping it as a part of the employees personnel file.

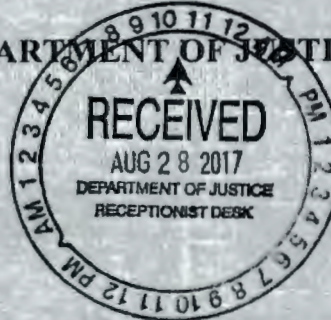
EXHIBIT

C



NAVAJO NATION DEPARTMENT OF JUSTICE

REQUEST
FOR
SERVICES



DOJ
8/28/17 10:16a
DATE / TIME
RFS #: 17-1036 #3
UNIT: H59w

☐ RESUBMITTAL

*** FOR NNDOJ USE ONLY - DO NOT CHANGE OR REVISE FORM. VARIATIONS OF THIS FORM WILL NOT BE ACCEPTED. ***

CLIENT TO COMPLETE

DATE OF REQUEST: 8/28/17 ENTITY/DIVISION: Dept. of Dir. Ad.
 CONTACT NAME: Brent Nelson DEPARTMENT: Dope
 PHONE NUMBER: 928-891-7475 E-MAIL: brennelson@navajo-nn.gov

COMPLETE DESCRIPTION OF LEGAL NEED AND SERVICES REQUESTED (attach documents):

Legal Review - Technology Policies.

DEADLINE:

REASON:

#64-Resub

DOJ SECRETARY TO COMPLETE

DATE/TIME IN UNIT: 8/28/17 1:25 REVIEWING ATTORNEY/ADVOCATE: Chris

DATE/TIME OUT OF UNIT: 8/30/17 2:25 PREPARED BY (initial):

DOJ ATTORNEY / ADVOCATE COMMENTS

Sufficient. I made a few notations.

REVIEWED BY: (PRINT)

Chris Schneider

DATE / TIME

30 Aug 17 / 1:57

DOJ Secretary Called:

Candace

for Document Pick Up on

8/30/17 at 2:25

By:

gm

PICKED UP BY: (PRINT)

DATE / TIME: