Office of the Controller

The Navajo Nation

Systems Policies Manual

Table of Contents

DESCRIPTION:	Systems	INDEX:	
	Financial Management Information System (FMIS) and Internet Usage	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements, 12 N.N.C. § 201, *et seq*

PURPOSE:

To establish policies that address proper FMIS and internet usage.

RESPONSIBILITY:

Office of the Controller (OOC) Supervisors and Managers

- Enforcement of the OOC Computer System Usage Policy.

POLICY:

This policy shall be used in accordance with the Navajo Nation (Nation) Personnel Policies and Procedures and shall apply to all employees of the OOC.

All OOC employees (Permanent/ Temporary) shall abide by the "OOC Computer System Usage Policy" (see attached). Any OOC employee requesting internet access shall receive a copy of this policy and acknowledge receipt and review via signature. No deviation or waiver of said policy shall be allowed. All violations shall be pursued in accordance with the Navajo Nation Personnel Policies Manual. Accounting managers are responsible for the enforcement, protection, and safeguarding of Nation equipment.

For the security of confidential and financial data, all Systems policies must be adhered to at all times. No waiver of these policies shall be given.

OOC Computer
Systems Usage Policy

DESCRIPTION:	Systems	INDEX:	
	Financial Management Information System (FMIS) System Maintenance Request	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements. 12 N.N.C. § 201, *et seq.*

PURPOSE:

To establish policies and procedures that address FMIS maintenance requests.

RESPONSIBILITY:

Office of the Controller (OOC) Systems Section

- Monitoring and implementation of System Maintenance Requests.

OOC Supervisors and Managers

- Approval of Systems Maintenance Requests.

POLICY:

The systems office periodically receives a request to shut down the FMIS to allow for corrections when no other users have access. The systems office shall monitor all requests and notify all users of the FMIS when maintenance will occur. All maintenance requests must be approved and properly tested before moving to the live environment.

DESCRIPTION:	Systems	INDEX:	
	Financial Management Information System (FMIS) Report Request	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements. 12 N.N.C. § 201, *et seq*

PURPOSE:

To establish policies and procedures that address report requests.

RESPONSIBILITY:

FMIS Report Writer

- Assess feasibility of report requests.
- Develop coding for report requests and testing of reports.

FMIS Power Users

- Approval of report requests.

POLICY:

The Office of the Controller (OOC) is responsible developing and testing requests for report generation. The OOC is responsible for tracking all requests and activities.

DESCRIPTION:	Systems	INDEX:	
	Financial Management Information System (FMIS) and Human Resource Information System Promotion Process for Object Management Workbench (OMW)	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements. 12 N.N.C. § 201, *et seq.*

PURPOSE:

To establish policies and procedures for promoting Custom Objects and Electronic Software Updates (ESU).

RESPONSIBILITY:

System Section

- Development, testing, and production of system updates.

POLICY:

The Office of the Controller (OOC) is responsible for maintaining a process for system modification, development, and patches. The OOC is responsible for proper testing and approval prior to promotion. In addition, the OOC is responsible for monitoring and tracking all FMIS activity and maintaining proper segregation of duties.

DESCRIPTION:	Systems	INDEX:	
	Financial Management Information System (FMIS) User Access and Termination of Access	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements. 12 N.N.C. 201, *et seq*

PURPOSE:

To establish policies and procedures that address access to the FMIS.

RESPONSIBILITY:

Office of the Controller (OOC) Supervisors and Managers

- Approval of user access and monitoring of timely termination of access.

POLICY:

This policy shall be used in accordance with the Navajo Nation Personnel Policies and Procedures and shall apply to all employees of the OOC. The OOC is responsible for only allowing access to the FMIS until successful completion of the FMIS training module. The OOC is responsible for removal or change in access for transferring or terminated employees.

DESCRIPTION:	Systems	INDEX:	
	Financial Management Information System (FMIS) System Idle Time	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements. 12 N.N.C. § 201, *et seq.*

PURPOSE:

To establish policies that address the FMIS idle time.

RESPONSIBILITY:

Office of the Controller (OOC) Supervisors and Managers

- Monitoring of appropriate security measures over the FMIS.

POLICY:

This policy shall apply to all Supervisors and Managers of the OOC.

- All OOC computer sessions should be locked when leaving the assigned work area. DO NOT LEAVE FMIS APPLICATIONS OPEN FOR SECURITY REASONS.
- Applications should not be open with confidential and propriety information available. PLEASE ENSURE THAT ALL SECURITY MEASURES ARE TAKEN WITH YOUR STAFF.
- Managers and Supervisors are required to walk and inspect on a routine basis their assigned sections to ensure Navajo Nation (Nation) data is safely protected.

To lock your computer workstation, press CONTROL, ALT, AND DELETE at same time and select Lock Computer. To reopen you will have type CONTROL, ALT, AND DELETE and enter your Citrix Password.

All OOC staff are not to use the save password feature for the FMIS. All staff are required to enter their passwords manually when logging into the FMIS.

It is up to the manager to enforce and protect Nation equipment/property.

For security of confidential and financial data all FMIS policies must be adhered to at all times. No waiver of these policies shall be given.

DESCRIPTION:	Systems	INDEX:	
	Financial Management Information System (FMIS) Standard Query Language (SQL) Request	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements. 12 N.N.C. § 201, *et seq.*

PURPOSE:

To establish policies and procedures that address SQL requests.

RESPONSIBILITY:

FMIS power users

- Completion of the SQL form and all supporting documentation.

Controller

- Approval of all SQL requests.

POLICY:

The Office of the Controller (OOC) will only allow SQL changes to data tables as a last resort. The OOC may consult with its information technology consultant prior to initiating an SQL change. Appropriate documentation must be maintained showing the measures taken prior to initiating an SQL change along with the approval of the Controller.

DESCRIPTION:	Systems	INDEX:	
	Password Update	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements. 12 N.N.C. § 201. *et seq.*

PURPOSE:

To establish procedures for the periodic update of passwords.

RESPONSIBILITY:

Office of the Controller (OOC) Employees

- Timely update of all passwords.

POLICY:

The OOC's policy is to require user passwords to be changed every three months. Computers will remind each user when the end of the three-month period approaches. Users will not be able to access their computers or cell phone if the three-month period elapses when a change of password.

DESCRIPTION:	Systems	INDEX:	
	Safeguarding of Assets	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements; 12 N.N.C. § 201, *et seq.*

PURPOSE:

To establish procedures for the safeguarding of assets.

RESPONSIBILITY:

Office of the Controller (OOC) Employees

- Safeguarding all property of the Navajo Nation (Nation).

OOC Managers

- Ensure all property is properly tagged by the Property Management Division (PMD)
- Safeguarding all property of the Nation.

POLICY:

Each department head is responsible for safeguarding all tangible and intangible assets purchased for his or her department and assisting with the physical inventory process. Physical security measures over assets should be established. Each department is responsible for ensuring assets are properly logged and tagged with the PMD (refer to Property Management Policy and Procedures). Each department is susceptible to internal and external audit verifications on a sample of capital assets.

Tangible Assets

Tangible assets are assets that have physical substance and are held for use in the production or supply of goods or services, for rental to others, or for administrative purposes on a continuing basis in the Nation's activities. For the purposes of this policy, tangible assets include, but are not limited to: fixtures, fittings, tools and equipment (i.e., computer equipment).

Intangible Assets

Intangible assets are those that lack physical substance and have an initial useful life extending beyond a single reporting period. Intangible assets must be identifiable, meaning they are either capable of being separated by means of sale, transfer, license or rent, or they arise from contractual or other legal rights. Intangible assets acquired or developed by the Nation could include licensed software, internally generated computer software and Nation owned websites or portals. Other examples include patents, copyrights and trademarks, permits and licenses, easements, and land use rights (e.g., water, timber or mineral rights).

DESCRIPTION:	Systems	INDEX:	
	Sensitive Electronic Information	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements; 12 N.N.C. § 201, *et seq.*; 2 N.N.C. § 85; Navajo Nation Personnel Policies Manual.

PURPOSE:

To protect the Navajo Nation's (Nation) sensitive electronic data from unauthorized disclosure and inappropriate use. Refer the "Office of the Controller – Sensitive Information and Privacy Act" policies and procedures for additional guidance.

RESPONSIBILITY:

Office of the Controller Employees

- Ensure all sensitive electronic information is appropriately secured.

POLICY:

The Nation's Sensitive Information policy requires that controls be in place to manage risk to the confidentiality, integrity and availability of sensitive data in any form and represent a minimum standard for protection of this data. Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health information, credit cardholder data, student), may also apply.

It is the responsibility of each individual with access to sensitive data resources to use these resources in an appropriate manner and to comply with all applicable federal, state, and local statutes. Additionally, it is the responsibility of each individual with access to sensitive data resources to safeguard these resources.

Sensitive Data:

Information intended for limited use within the Nation that, if disclosed, could be expected to have a serious adverse effect on the operations, assets, or reputation of the Nation, or the Nation's obligations concerning information privacy. Sensitive information is data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.

There are three main types of sensitive information:

1. **Personal information:**

Sensitive personally identifiable information (PII) is data that can be traced back to an individual and that, if disclosed, could result in harm to that person. Such information includes biometric data, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Social Security numbers. Threats include not only crimes such as identity theft but also disclosure of personal information that the individual would prefer remained private. Sensitive PII and PIFI should be encrypted both in transit and at rest.

2. **Business information:**

Sensitive business information includes anything that poses a risk to the company in question if discovered by a competitor or the general public. Such information includes trade secrets, acquisition plans, financial data and supplier and customer information, among other possibilities. With the ever-increasing amount of data generated by businesses, methods of protecting corporate information from unauthorized access are becoming integral to corporate security. These methods include metadata management and document sanitization.

3. **Classified information:**

Classified information pertains to a government body and is restricted according to level of sensitivity (for example, restricted, confidential, secret and top secret). Information is generally classified to protect security. Once the risk of harm has passed or decreased, classified information may be declassified and, possibly, made public.

Refer to 2 N.N.C. § 85 for examples of sensitive information.

Employees are reminded that disclosing confidential information to unauthorized person(s) may result in termination from employment. See the Navajo Nation Personnel Policy Manual, Section XIII, Part G, *Table of Penalties*.

DESCRIPTION:	Systems	INDEX:	
	Incident Response Plan	POLICY:	X
		PROCEDURES:	
		EFFECTIVE DATE:	

LEGAL AUTHORIZATION: System Audit Requirements; 12 N.N.C. § 201, *et seq.*; 2 N.N.C. § 85; Navajo Nation Personnel Policies Manual.

PURPOSE:

To guide the Navajo Nation in responding to an incident.

RESPONSIBILITY:

Systems Section

- To develop and implement an appropriate incident response plan.

Office of the Controller (OOC) Employees

- To comply with the incident response plan developed by the systems section.

POLICY:

An "Incident" means a cyberattack or other systems malfunction or outage with respect to an OOC computer or other electronic systems (an OOC "Incident"), or the computer or other electronic systems of a counterparty, vendor, exchange, trading platform, bank or governmental entity (an "Affected Third Party Incident") or any other similar event that threatens to cause material damage to the OOC's business, financial condition, or reputation, or the OOC's ability to operate its business.

This Plan is intended to provide guidance for incidents anywhere in the world.

This Plan is part of the NNOOC's Cyber Security Framework, which consists of five Core Elements:

1. Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. Protect: Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.
3. Detect: Develop and implement the appropriate activities to identify the occurrence of an incident.
4. Respond: Develop and implement the appropriate activities to take action regarding a detected incident.
5. Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an Incident.

It is difficult to formulate an emergency response plan that has a clear set of actions relevant for all situations. Decisions must be made on a case by case basis as dictated by the Incident. When confronted with an Incident, the Nation generally seeks to:

- Contain the Incident
- Minimize the impact of the Incident
- Remediate impacted systems or develop workarounds
- Comply with legal requirements
- Reduce the Nation's liability exposure.

The OOC headquarters in Window Rock, AZ will assume primary command, control, and communications responsibilities regardless of the location of the Incident.

BUDGET AND FINANCE COMMITTEE

21 January 2020

Regular Meeting

VOTE TALLY SHEET:

Legislation No. 0002-20: An Action Relating to Budget and Finance Committee; Rescinding Resolution BFJY-114-186, Relating to the use of proceeds from the sale of Tribal Vehicles and BFD-37-14, Relating to Purchase Card Policies; Amending Resolution BFJA-01-02, Relating to Employee Travel Policies and Procedures; Approving the Policies of the Navajo Nation Office of the Controller *Sponsored by Jamie Henio, Council Delegate*
Motion: Amber K. Crotty
Second: Elmer P. Begay
Vote: 4-0, Vice Chairman not voting

Vote Tally:

Jamie Henio	**yea**	
Jimmy Yellowhair		
Raymond Smith Jr.		
Elmer P. Begay	**yea**	
Amber K. Crotty	**yea**	
Nathaniel Brown	**yea**	

Absent: Jimmy Yellowhair

Raymond Smith, Jr., Chairman
Budget & Finance Committee

Peggy Nakai, Legislative Advisor
Budget & Finance Committee