

CJY-34-92

Class "C" Resolution
No BIA Action Required.

RESOLUTION OF THE
NAVAJO NATION COUNCIL

Mandating the Creation of an Open Information Environment Among
the Governmental Entities of the Navajo Nation Government; and to
Assign Responsible Parties to Coordinate the Use and
Development of Computer Technology to Accomplish the
Open Information Sharing Environment.

WHEREAS:

1. Pursuant to 2.N.T.C., Section 102 (a), the Navajo Nation Council is the governing body of the Navajo Nation; and

2. The Navajo Nation Council wishes to declare the following General Policy on Ownership of Government Data and Information:

Data and information that is gathered, processed, created and manipulated in support of Navajo Nation government operations or during the course of conducting Navajo Nation Government business belongs to the Navajo Nation Government and shall be shared throughout the governmental system. It is also acknowledged that the sharing of governmental information may be restricted where necessary and that information processing activity within the Navajo Nation is to be conducted in a secure environment.

3. The Navajo Nation Council wishes to declare the following General Policy on Use and Development of Computer Technology to Accomplish the Open Information Environment.

It is understood that through the use of modern management techniques and computer technology it is possible to promote the sharing of data and information throughout the Navajo Nation Government including the chapter level. It is further understood that the concept of distributed processing can be used to accomplish the establishment of an overall computer information strategy. However, it is also understood that any distribution of processing such as financial transactions through the use of computers must be carefully analyzed and planned prior to implementation.

4. It is in the best interest of the Navajo Nation that government operations be supported by an effective and efficient framework for improving the timeliness, accuracy and availability of data and information resources. The open information environment will help achieve this end.

NOW THEREFORE BE IT RESOLVED THAT:

1. The Navajo Nation Council hereby declares a General Policy on ownership of government data and information as defined below:

Data and information that is gathered, processed, created and manipulated in support of Navajo Nation government operations or during the course of conducting Navajo Nation Government business belongs to the Navajo Nation Government and shall be shared throughout the governmental system. The specifics of the open information environment are contained in the Open Information Policy attached hereto as Attachment 1.0-A-1 and by reference made a part hereof;

It is also acknowledged that the sharing of governmental information may be restricted where necessary and that information processing activity within the Navajo Nation is to be conducted in a secure environment. The degree of this security will be governed by two principles. First, the security must be consistent with applicable federal, state and Navajo Nation laws, regulations and directives. Secondly, security must be commensurate with the value of the data and physical facilities considering loss/value to the Tribe. The Data Security Policy attached hereto as Attachment 1.0-B-1 covers these areas in greater detail.

2. The Navajo Nation Council further hereby declares a General Policy on use and development of computer technology to accomplish the open information environment.

It is understood that through the use of modern management techniques and computer technology it is possible to promote the sharing of data and information throughout the Navajo Nation Government including the Chapter level. It is further understood that the concept of distributed processing can be used to accomplish the establishment of an overall computer information strategy. However, it is also understood that any distribution of processing such as financial transactions through the use of computers must be carefully analyzed and planned prior to implementation.

3. The Navajo Nation Council further hereby mandates:

1. The declaration of the Open Information Sharing Environment to be effective immediately; and
2. The implementation of an Overall Computer Information Strategy for the Navajo Nation to be addressed immediately as outlined hereinafter; and as set forth in the attachments; and
3. The accomplishment of the Distributed Processing of selected Financial Transactions to the Agency level of Government via Computer Technology by the end of Fiscal Year 1993; and
4. The accomplishment of Chapter Government access to various Government data and information via computer technology by the end of Fiscal Year 1994 or sooner.

4. The Navajo Nation Council further hereby establishes the Standards Group, Data Guardian, Data Security Manager, Inter-branch Project Team, the Information Management Centers Steering Committee and structure to accomplish the above tasks outlined in Resolved Clause, Paragraph 3.

1. The Standards Group will coordinate and facilitate strategic planning, coordinate technology acquisitions and directions by establishing and maintaining technology standards, keep respective Branch chiefs abreast of the information issues; and to resolve information/technology issues and concerns as they are brought forth by the Data Guardian, Data Security Manager, Project Staff, Work Groups and other parties. The Standards Group will be comprised of the following voting members

1. The President representing the Executive Branch shall appoint one person from the Division of Finance and one at-large member to represent the Executive Branch;
2. The Speaker of the Navajo Nation Council representing the Legislative Branch shall appoint two persons from his office to represent the Legislative Branch;
3. The Chief Justice of the Supreme Court representing the Judicial Branch shall appoint two persons from his office to represent the Judicial Branch;

4. The Data Guardian will serve as the Chairperson of the Group;
5. The Data Security Manager;
6. The Chairpersons of various user group organizations, the Navajo Macintosh User Group, the VAX Site Managers and the Chairperson of the local DECUS LUG. Other organizations can petition the Chairperson and can be included with a two-thirds majority of the voting members.
7. Representatives of strategic partnering organizations, who provide a significant amount of product, services or expertise and require close coordination with the Tribe, will be included as non-voting resource members. Other organizations can petition the Chairperson and can be included with a two-thirds majority of the voting members.

2. The Information Technology Coordinator, Office of the Speaker is designated as the Data Guardian to implement the Open Information Environment and chair the Standards Group on behalf of the Navajo Nation Council.

3. The Director, Department of Information Management Services is designated as the Data Security Manager to safeguard the Open Information Environment on behalf of the Navajo Nation Council.

4. The assignment of technical support staff will be necessary to successfully implement an open information sharing environment. Therefore, the Department of Information Management Services (or its successor in function and operation) will be given the task of supporting the project by implementing programming modifications, providing system analysis functions, assist in recommending connectivity requirements and other technical activities.

5. The following work groups will be established with a representative cross section from each Branch to address the distributed financials question until a more permanent solution can be agreed upon.

1. Operations Work Group to review and evaluate procedural issues and concerns to be addressed in order to carry out the Open Information Environment. They shall, in consultation with the appropriate operational managers and chapter level representatives

assess the type of data and information to be shared with the Chapter level government and determine the distributed processing needs for financial transactions to be accomplished at the Agency level of government.

2. Policy Work Group to review and evaluate policy issues and concerns to be addressed, changed, created or deleted in order to carry out the mandates of the Navajo Nation Council. They shall in consultation with the other work groups formulate legislation and/or policy to carry out the Open Information Environment.

3. Technology Work Group to review and evaluate automation issues and concerns to be addressed in order to carry out the Open Information Environment. They shall, in consultation with the other work groups formulate the plans for technology developments necessary to carry out the Open Information Environment.

6. The Information Management Centers Steering Committee's primary goal is to provide an ongoing forum to coordinate government-wide automation activities to ensure current standards adherence and the productive and cost effective use of technology in meeting day to day governmental information needs. In addition, the IMCSC will be able to provide input on the adoption of new standards, as well as provide an alternative channel for challenging adopted standards.

1. The IMCSC will be comprised of representatives from all Branches who are responsible for the day to day operations of information areas. Membership is non-formal and open to anyone who works with information or information technologies.

2. The IMCSC will assist with the coordination of purchasing, network planning, implementation of technology, support the Standards Group, the Data Guardian and the Data Security Manager with recommendations and insights on technical issues and concerns.

5. The Navajo Nation Council further hereby directs all Branches, Divisions, Departments, Offices, Programs and other tribal entities to cooperate to the fullest extent possible to carry out the above mandates.

6. The Navajo Nation Council further hereby directs that a report on the progress made in carrying out the above policy and mandates be made in writing by the Office of the Speaker at each session of the Navajo Nation Council hereinafter until such time that the provisions of this policy and resolution have been accomplished.

CERTIFICATION


I hereby certify that the foregoing resolution was duly considered by the Navajo Nation Council at a duly called meeting at Window Rock, Navajo Nation (Arizona), at which a quorum was present and that same was passed by a vote of 69 in favor, 6 opposed and 0 abstained, this 23rd day of July 1992.


Speaker
Navajo Nation Council

July 28, 1992
Date Signed

ACTION BY THE EXECUTIVE BRANCH

- 1. Pursuant to 2 N.T.C., Section 1005 (c)(1), I hereby sign into law the foregoing legislation on this 30 day of July 1992:


Peterson Zah, President
Navajo Nation

* * * *

- 2. Pursuant to 2 N.T.C., Section 1005 (c)(10), I hereby veto the foregoing legislation this ___ day of ___ 1992 for the reason(s) expressed in the attached letter to the Speaker:

Peterson Zah, President
Navajo Nation

ATTACHMENT 1.0-A-1

Open Information Policy

A. PURPOSE

To create an environment that will facilitate the productive use of information among all governmental entities of the Navajo Nation government and to coordinate the use and development of computer technology to accomplish an open information sharing environment.

B. SCOPE

The policy will cover all Navajo Nation data and information and will be binding on all Navajo Nation branches, divisions, departments, programs, entities, chapters, and other sub-units of the Navajo Nation and their employees; all persons, both Navajo Nation government and Non-Navajo Nation government, who have a germane need to utilize data with the exception of those which are specifically restricted by federal, state or Navajo Nation laws, regulations and directives.

C. STATEMENT OF POLICY

1. Data and information that is gathered, processed, created and manipulated in support of Navajo Nation government operations or during the course of conducting Navajo Nation Government business belongs to the Navajo Nation, and should be shared throughout the governmental system.
2. All information used in the course of Navajo Nation business is an asset and as such, the Navajo Nation Government entities are responsible and accountable for its protection.
3. It is understood that through the use of modern management techniques and computer technology it is possible to promote the sharing of data and information throughout the Navajo Nation Government including those at the Chapter level.
4. It is further understood that the concept of "distributed processing" can be employed through the establishment of an overall computer information strategy. However, it is also understood that any such distribution of data processing through the use of computers must be carefully analyzed and planned prior to implementation.

D. AUTHORITY AND RESPONSIBILITY

1. The coordination of the study, design, implementation, and support of data sharing activities and directions is important to the overall implementation of the Navajo Nation's Information Strategy. The "Data Guardian" will implement the Information Strategy in collaboration with the three branches to meet the information needs of the Navajo Nation Government. The following cross

- a. The Standards Committee shall maintain and update technology standards as stated in the Navajo Computing Environment Specifications (NCES). The Committee will review all automation guidelines for system procurement, network standards, equipment specifications, regulations, policies and procedures to ensure the efficient and coordinated utilization of technology and techniques to achieve optimum productivity. This committee deals with the long term information goals of the tribal government.
- b. The Information Management Centers Steering Committee's (IMCSC) primary goal is to provide an ongoing operational forum to coordinate government-wide automation activities to ensure current standards adherence and the productive and cost effective use of technology in meeting day to day governmental information needs. In addition, the IMCSC will be able to give input on the adoption of new standards, as well as, provide an alternative channel for challenging adopted standards.
- c. It is further anticipated that an entity will need to be established or delegated to provide for the efficient and coordinated utilization of technology equipment, techniques and personnel to achieve optimum effectiveness, economy and productivity in the collection, storage, interchange, retrieval, processing, transmission and security of information.

This entity shall develop, implement and maintain a coordinated Navajo Nation wide information strategy for automation and network (data communications) structures, including the establishment of operation centers, for the purpose of serving the management and other needs of the legislative, executive and judicial branches of the Navajo Nation.

This entity shall promulgate rules, regulations, policies and procedures applicable to all tribal departments relating to the coordination and the acquisition of automated equipment, techniques and services.

E. NON-COMPLIANCE

The ability of the Navajo Nation to provide improved services to the Navajo People is founded on the Nation's ability to share data, resources and information. Failure to adhere to the intent of the Open Information Policy may result in the loss of a department's Information Management Center status and/or individual disciplinary action for neglect of duty.

ATTACHMENT 1.0-B-1**Data Security Policy****A. PURPOSE**

To provide guidelines and define responsibilities with respect to the protection of information and processing of data to ensure against loss, unauthorized modification, improper destruction, misuse or unauthorized disclosure of data whether accidental or intentional. This includes the protection of Navajo Nation data, computer hardware and software from accidental damage, unauthorized access, improper storage, theft, fire, flood, wind or any natural or man-made disaster.

B. SCOPE

This policy encompasses all Navajo Nation data, all Navajo Nation personnel; all persons, both Navajo Nation government and Non-Navajo Nation government (i.e. consultants, etc.), who have access to Navajo Nation data in the performance of their duties; and all persons, Navajo Nation and Non-Navajo Nation, who have responsibility for maintaining and preserving Navajo Nation data.

C. STATEMENT OF POLICY

1. All information used in the course of Navajo Nation business is an asset and as such, elected officials, directors (Executive, Division, Department and Program), employees, and other tribal officials are responsible and accountable for its protection and for the use of said data only for official purposes.
2. Data processing activity within the Navajo Nation is to be conducted in a secure environment. The degree of this security will be governed by two principles. First, the security must be consistent with applicable federal, state and Navajo Nation laws, regulations, and directives. Secondly, security must be commensurate with the value of the data and the physical facilities considering loss/value to the tribe.
3. The data-sharing policy provides for two objectives: the protection of data and the controlled sharing of data. Data maintained by Information Management Centers within the three Branches may be shared only with those individuals or entities who have established a need for access (need to know) based upon applicable federal, state, and Navajo Nation laws, regulations and directives.
4. Measures must be established to ensure the integrity, accuracy and confidentiality of data.
5. Measures must be established to ensure that cost-effective, current, proven contingency plans, exist for dealing with emergencies, disasters and minor incidents.

ATTACHMENT 1.0-B-1**Data Security Policy****A. PURPOSE**

To provide guidelines and define responsibilities with respect to the protection of information and processing of data to ensure against loss, unauthorized modification, improper destruction, misuse or unauthorized disclosure of data whether accidental or intentional. This includes the protection of Navajo Nation data, computer hardware and software from accidental damage, unauthorized access, improper storage, theft, fire, flood, wind or any natural or man-made disaster.

B. SCOPE

This policy encompasses all Navajo Nation data, all Navajo Nation personnel; all persons, both Navajo Nation government and Non-Navajo Nation government (i.e. consultants, etc.), who have access to Navajo Nation data in the performance of their duties; and all persons, Navajo Nation and Non-Navajo Nation, who have responsibility for maintaining and preserving Navajo Nation data.

C. STATEMENT OF POLICY

1. All information used in the course of Navajo Nation business is an asset and as such, elected officials, directors (Executive, Division, Department and Program), employees, and other tribal officials are responsible and accountable for its protection and for the use of said data only for official purposes.
2. Data processing activity within the Navajo Nation is to be conducted in a secure environment. The degree of this security will be governed by two principles. First, the security must be consistent with applicable federal, state and Navajo Nation laws, regulations, and directives. Secondly, security must be commensurate with the value of the data and the physical facilities considering loss/value to the tribe.
3. The data-sharing policy provides for two objectives: the protection of data and the controlled sharing of data. Data maintained by Information Management Centers within the three Branches may be shared only with those individuals or entities who have established a need for access (need to know) based upon applicable federal, state, and Navajo Nation laws, regulations and directives.
4. Measures must be established to ensure the integrity, accuracy and confidentiality of data.
5. Measures must be established to ensure that cost-effective, current, proven contingency plans, exist for dealing with emergencies, disasters and minor incidents.

D. AUTHORITY AND RESPONSIBILITY

1. The authority and responsibility to enact security controls are derived from federal, state and Navajo Nation laws, regulations and directives.
2. The Data Security Manager is responsible for all data security related matters including: conducting security audits, development of security standards, implementation of standards, development of security training programs, investigation and tracking of security breaches with recommendations of corrective action, to stay apprised of legislative directives impacting security and to disseminate information regarding new and updated security policies.
3. Each Navajo Nation employee is responsible for safeguarding data and ensuring that data is not misused or obtained by unauthorized persons.
4. Employees, users, custodians, data managers, and owners of Navajo Nation data are prohibited from:
 - a. Revealing Navajo Nation data to persons within or outside the Navajo Nation who have not been specifically authorized to receive such data.
 - b. Attempting or achieving access to Navajo Nation data not germane to mandated job duties or outside authorized access agreements.
 - c. Entering/altering/erasing Navajo Nation data for direct or indirect personal gain or advantage.
 - d. Entering/altering/erasing Navajo Nation data maliciously or in retribution for real or imagined abuse, or for personal amusement.
 - e. Using Navajo Nation terminals, workstations, printers and/or other equipment for other than work-related purposes.
 - f. Using another person's data access control identifier and password.
 - g. Revealing their personal Navajo Nation account and/or password to another person.
 - h. Asking another user to reveal his/her personal Navajo Nation account and/or password.
 - i. Making any exceptions to the Navajo Nation Security Policy without prior approval from the Data Guardian and the Data Security Manager.

E. BREACHES OF SECURITY

Appropriate action will be taken to ensure that applicable federal, state and Navajo Nation laws, regulations and directives governing security are enforced. A breach of procedures occurring pursuant to this policy or misuse of department property including computer programs, equipment and/or data may result in disciplinary action including dismissal, and/or prosecution.

F. DATA RESPONSIBILITY CLASSIFICATIONS

1. Data owners, guardians, custodians and users have a shared responsibility to ensure data protection. Access to Navajo Nation data shall be assigned to respective job functions, not to individuals.

a. DATA OWNERS

The Navajo Nation Council, pursuant to 2 NTC Section 102(a), is the

Governing body of the Navajo Nation, and will act as the owner of all governmental data. The government as a legal entity retains the exclusive right and use of all information assets in accordance with applicable federal, state and Navajo Nation laws, regulations and directives.

b. DATA GUARDIAN

The person primarily responsible for the coordination and implementation of the Open Information Environment. The Guardian will represent the Navajo Nation Council in regards to policy and procedural questions.

c. DATA MANAGERS

Directors and managers of a program in which the data originates. Person(s) primarily responsible for the accuracy and integrity of data.

d. DATA CUSTODIAN

The managers of data-processing operations, distribution operations, storage operations, and contractors who process, distribute or store data shall be designated custodians of the data. Data custodians assume responsibility for maintaining the data in the care of their organization. The release of data maintained by the data custodians may only occur if authorization is received from the data owner. Person(s) responsible for the information assets while under his control.

e. DATA USER

Any person or organization which requires, manipulates, further processes and/or disseminates data shall be designated a user of that data.

G. SHARING OF DATA

1. Data-sharing agreements must be initiated among the Data Managers, Custodians and entities outside the Navajo Nation who have established a need for access to data owned by another program or entity with the collaboration of the Data Guardian. Approval for access shall be based upon provisions of federal, state and Navajo Nation laws, regulations and directives governing security and confidentiality.
2. Re-disclosure of information is prohibited without formal consent from the originating source.

H. INDIVIDUAL RECORD REVIEW

Access and review of a person's own individual records including client data, provider data and personnel data will be permitted in accordance with federal, state and Navajo Nation laws, regulations and directives governing confidentiality.

I. SOFTWARE DEVELOPMENT AND ACQUISITION

This policy governs all software and specifically addresses purchasing, developing and maintaining software applications. Each software application will be evaluated in terms of its compatibility with established security controls. No software shall bypass or interfere with these security controls. Such controls may include use of data encryption software.

passwords and/or physical security controls.

J. COMMUNICATIONS SECURITY

Protection for telecommunications must comply with federal, state and Navajo Nation regulations.

K. DEFINITIONS

1. **ACCESS** - the obtaining or viewing of data; the ability and the means to approach, store or retrieve data, to communicate with, or to make use of any resource.
2. **BREACH** - a violation of state or federal security laws or regulations; or a violation of Navajo Nation security policies and/or procedures.
3. **CONFIDENTIALITY** - a term that refers to data whose unauthorized disclosure could be prejudicial to the Nation, the department, its personnel, its providers or its clients.
4. **DATA-ACCESS CONTROLS** - administrative measures employed, and the tasks performed by hardware and software to monitor system operations, ensure data integrity, perform user identification, record system access and changes, and grant user access.
5. **DATA INTEGRITY** - the preservation of data or programs for their intended purpose. The state that exists when computerized data is the same as the source documents and has not been exposed to accidental or malicious alteration or destruction.
6. **GERMANE** - relevant and appropriate
7. **HARDWARE** - the computer and all related or attached machinery, such as mechanical, magnetic, electrical, and electronic devices used in data processing.
8. **PASSWORD** - a unique word or string of characters that a program, computer operator or user must supply to meet security requirements before gaining access to data.
9. **PRIVACY** - the right of individuals and organizations to control the collection, storage and dissemination of their data or information about themselves.
10. **SAFEGUARDING** - providing precautionary measure, stipulations or technical contrivances to prevent security exposures.
11. **SOFTWARE** - a set of computer programs, procedures; and associated documentation concerning the operation of a computer system.
12. **STORAGE** - a facility used for housing data or computer programs and retaining them for subsequent use.