NORTH Dakota Be Legendary.

State of North Dakota
IT Standards

Date: 2025-07-11

Table of Contents

Acceptable Use of Electronic Communication Devices Standard

Purpose

To ensure the responsible and effective use of Electronic Communications Devices (ECDs).

Standard

North Dakota state government branches and agencies are responsible for developing and administering policies to prevent or detect abuse and reduce legal exposure related to the use of ECDs.

Definition

Electronic Communication Device - Telephones, desktop computers, laptop computers, tablet computers, facsimile (fax) machines, video equipment, and all computer and network-related hardware.

Guidance

The following are examples that can be used by agencies to develop their own policy

1. Office of Management and Budget – Universal HR Polices: Electronic Communication Devices
   IT Policies:
   1. Artificial Intelligence Policy
   2. Data Classification Policy

Policy

The purpose of this standard is to require all who use the state's IT infrastructure to develop a policy that ensures the appropriate use of ECDs.

Applicability

North Dakota Century Code 54-59-09

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Revision History

Date	Authored by	Approved by	Version	Description of Change
02/26/2025	NDIT	NDIT Management	1.0	Creation of Standard
3/11/2020	NDIT	NDIT Management	1.1	Annual Review
04/29/2021	NDIT	NDIT Management	1.2	Annual Review
08/09/2022	NDIT	NDIT Management	1.3	Annual Review
04/06/2023	NDIT	NDIT Management	1.4	Annual Review
11/06/2024	NDIT	NDIT Management	1.5	Annual Review
04/29/2025	NDIT	NDIT Management	1.6	Updated Guidance Links

Number: POL0020032
Revision Number: 1.6
Revision Date: 2024-04-29
Effective Date: 2013-06-09
Last Reviewed: 2024-04-29

Access Control Standard

Purpose

To establish login and password procedures for access to all servers, workstations, and network-attached devices (where applicable) thereby ensuring the reliability, accessibility, and security of such devices.

Standard

REDACTED - Contact NDIT for more information

Number: POL0020034
Revision Number: 1.7
Revision Date: 2025-06-17
Effective Date: 2004-12-08
Last Reviewed: 2025-06-17

Accessibility Standard

Purpose

Improve the accessibility and usability of information technology products and services for all State of North Dakota government end-users.

Standard

Web Content Accessibility Guidelines (WCAG) Version 2.1, Level AA is the technical standard for web content and mobile applications.

Definition

Web Content - Text, visual, or audio content made available online, including content in a web-based application.

Mobile Application - An application made available for use on a mobile device.

Applicable North Dakota Century Code (NDCC)

For accessibility information - Refer to NDCC 14-02.4-14 and NDCC 14-02.4-15 for definitions of discrimination in the provision of public services.

Guidance

1. Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments
2. Web Content Accessibility Guidelines (WCAG) 2.1

Policy

Digital content, websites, applications, tools, and technologies are designed and developed so that people with disabilities can use them.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0030001
Revision Number: 1
Revision Date: 2024-11-14
Effective Date: 2025-01-01
Last Reviewed: 2024-11-14

Accounts Payable Standard

Purpose

Standardize the solution to provide the enterprise with the ability to manage accounts payable.

Standard

1. PeopleSoft Financials and Supply Chain Management (FSCM) from Oracle; will be used to fulfill accounts payable business needs.

Definitions

Accounts Payable - Accounts payable is money owed by by the State to its suppliers shown as a liability on the States balance sheet.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020173
Revision Number: 1
Revision Date: 2021-04-06
Effective Date: 2021-04-06
Last Reviewed: 2024-09-13
```

Accounts Receivable Standard

Purpose

Standardize the solution to enable the enterprise to manage Accounts Receivable.

Standard

1. PeopleSoft Financials and Supply Chain Management (FSCM) from Oracle; will be used to fulfill accounts receivable business needs.

Definitions

Accounts Receivable - Accounts receivable (AR) is the balance of money due to a firm for goods or services delivered or used but not yet paid for.

PeopleSoft Financials and Supply Chain Management (FSCM) - PeopleSoft module for managing credit, collections, deductions, and disputes, in addition to core receivables processes and ensuring compliance with accounting guidelines.

Scope

This standard applies to all executive branch state agencies, including the University Systems Office but excluding other higher education institutions, i.e., campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020172
Revision Number: 1
Revision Date: 2021-04-06
Effective Date: 2021-04-06
Last Reviewed: 2024-09-13

Active Directory Standard

Purpose

To coordinate Active Directory in the state of North Dakota which will establish a single network domain that provides users with a single network sign on, offers push technology for the distribution of applications, and allows for distributed management of computing process.

Standard

1. Any agency computers utilizing Active Directory shall be members of the state forest NDGOV
2. Each agency shall comprise an Organizational Unit (OU) within NDGOV.

Policy

The state of North Dakota shall establish a single forest architecture for its Active Directory. All state agency networks using Active Directory shall coordinate their installation and maintenance activities with ITD to ensure that all networked Active Directory computers are members of the State forest, NDGOV.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020116
Revision Number: 2
Revision Date: 2016-06-22
Effective Date: 2004-05-11
Last Reviewed: 2024-09-13

Administrative User Credential Management Standard

Purpose

Standardize the solution to provide the enterprise with the ability to securely store administrative user passwords and other secret keys for retrieval.

Standard

1. PasswordState provided by Click Studios; will be used to fulfill our credential management business needs.

Definitions

Credential - Credentials are typically a username and password combination used for logging.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020194
Revision Number: 1
Revision Date: 2021-05-13
Effective Date: 2021-05-13
Last Reviewed: 2024-09-13
```

Auditing Standard

Purpose

To ensure basic auditing requirements are in place to meet enterprise auditing needs.

Standard

1. For state hosts or new applications on a state host that require users to log on, auditing shall be activated to capture
   - all logon successes and failures
   - all security administration functions

   For state firewalls and DHCP servers, auditing shall be activated to capture

   - network firewall transactions
   - ip address logs (DHCP)
3. Audit records shall be retained for a minimum of ninety (90) days.
4. Audit records shall be documented on the owning agency's records retention schedule.

Definition

Security Administration Functions - Functions that change the security of a system. Functions include but are not limited to: creating, changing, deleting login ids; granting or revoking access privileges; changing security configuration values that affect audit logging, logons/logoffs, passwords.

State Hosts - Computers that are owned/operated by a state agency that provide the function of sharing resources such as files or records within files, or services with one or more computers.

Applications - Computer programs that provide a function for a customer. Computer operating systems (OS's) are not included as applications. They are part of the host definition.

Guidance

Current applications should be reviewed and logging should be activated if supported.

Policy

To provide a common auditing practice to aid in troubleshooting when needed and to be able to provide proof of access permissions.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020117
Revision Number: 1
Revision Date: 2005-07-18
Effective Date: 2005-07-18
Last Reviewed: 2024-09-13

Authentication, Public Standard

Purpose

Standardize public digital identity management to enhance customer service by simplifying access to state online services.

Standard

1. Applications that provide authenticated public access to state on-line services shall use the State of North Dakota Login service.
2. Applications shall not require users to have more than one State of North Dakota Login user account.

Definitions

Application - A software solution that accomplishes one or more business processes.

Authenticated Public Access - The act of verifying and granting a user access to one or more online services via the persisted identifier.

Public - An entity, including but not limited to citizens, private businesses, non-profit organizations, etc.

State of North Dakota Login Service - The State's centralized public identity service consisting of both managed and trusted federated identity provider functionality.

Policy

Applications providing public access to online state services must integrate with the State of North Dakota Login service, ensuring consistent digital identity management and seamless user experiences.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Appendix A - State of North Dakota Login Service

State of North Dakota Login serves as the State's centralized public identity management service for citizens and non-state entities. It enables secure and efficient access to state services and applications by offering centralized account management and self-service capabilities.

State of North Dakota Login Service Capabilities:

- Self-service account creation and management.
- Single Sign-On (SSO) - A user authentication process that permits a user to access multiple applications with one set of login credentials. SSO enhances user experience by reducing the need for multiple usernames and passwords while maintaining security through centralized identity management.
- OpenID Connect (OIDC) - A standardized protocol used to integrate applications with an identity service, allowing verification of user identities and access to basic profile information.

Number: POL0020022
Revision Number: 2
Revision Date: 2025-06-02
Effective Date: 2021-04-01
Last Reviewed: 2025-06-02

Authentication, State Entity Standard

Purpose

Standardize State entity digital identity management to support enhanced reuse and security.

Standard

1. All State entities will use the State's managed instance of Microsoft Entra ID for digital identity management.

Definitions

Digital Identity Management - A wholistic set of identity related activities, including but not limited to identity proofing, authentication and use of authenticators, and identity federation.

State Entity - A state entity means any state official, state employee or other person authorized to act on behalf of the state or any named service or device directly managed by the state.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020021
Revision Number: 2
Revision Date: 2025-06-02
Effective Date: 2021-04-01
Last Reviewed: 2025-06-02

Bidirectional Forwarding Detection (BFD) Standard

Purpose

To detect faults between two forwarding engines connected by a link. This enables an endpoint site with redundant paths or point to multi-point to core locations to fail over quicker and also allows core sites that are multi-point to other cores to detect failures quicker. This includes both IPv4 and IPv6.

Standard

1. NDIT utilizes BFD to mitigate network outages where appropriate.
2. Approved Vendor(s):
   - NDIT controlled Juniper and Palo Alto equipment.

Scope

This standard applies to all STAGEnet entities.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020057
Revision Number: 1
Revision Date: 2021-04-01
Effective Date: 2021-04-01
Last Reviewed: 2024-09-13

Contact Center Standard

Purpose

Standardize the solution to provide the enterprise with the ability to manage a contact center.

Standard

1. Genesys Cloud will be used to fulfill the business needs of a contact center.

Definitions

Contact Center *- Call center is a centralized service used for receiving and/or transmitting incoming enquiries. This can include phone, email, sms or chat.*

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020210
Revision Number: 2
Revision Date: 2025-01-07
Effective Date: 2021-07-20
Last Reviewed: 2025-01-07
```

Data Classification Standard

Purpose

Data classification establishes a common labeling model based on potential risk. The risk level is determined by assessing the impact on the state or its citizens from the unauthorized access, modification, or destruction of data.

Standard

1. All data under the stewardship or ownership of the state shall be classified classified into one of three classes: 1) **Low Risk**, 2) **Moderate Risk**, or 3) **High Risk**.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Policy

The purpose of the Data Classification Policy is to ensure that data is classified and handled consistently and securely, and that all employees understand their roles and responsibilities with respect to data protection. The policy specifies the categories and criteria for classifying data and a reference model of the protection controls for each category.

```
Number: POL0020146
Revision Number: 1
Revision Date: 2024-09-13
Effective Date: 2024-09-13
Last Reviewed: 2024-09-13
```

Database Standard

Purpose

Reduced total cost of ownership while increasing efficiencies in data sharing, data integrity, database support, and training.

Standard

1. All new applications shall use databases specified in the "Supported Databases" list. New databases will be presented to the Data Architecture team for review and evaluation. The list will be updated accordingly.
2. If data for new applications require features of an Enterprise Database, the application must utilize an Enterprise Database.

Definition

1. ***New Applications*** - New application software or replacement of existing application software, including all custom developed software, vendor software, and off-the-shelf software. Maintenance or enhancements to an existing application are not considered new applications.

   Enterprise Database definition:

   - Ability to scale to a large number of users
   - Provides data integrity, meaning the data in the database is consistent and accurate.
   - Provides support for industry standards (i.e. ANSI SQL-2011, ODBC, JDBC and XML).
   - Provides for security of the data.
   - Provides built-in audit capabilities.
   - Provides point in time recovery.
   - Provides backup and recovery utilities.
   - Provides logging for backup, recovery, and auditing.
   - Provides support large objects (BLOBS, CLOBS, etc.)

     Provide the basic properties of a database transaction: (ACID) Atomicity, Consistency, Isolation, and Durability

     - Atomicity - The entire sequence of actions must be either completed or aborted. The transaction cannot be partially successful.
     - Consistency - The transaction takes the resources from one consistent state to another.
     - Isolation - A transaction's effect is not visible to other transactions until the transaction is committed.
     - Durability - Changes made by the committed transaction are permanent and must survive system failure.

Policy

Databases will be consistent across the Enterprise.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Appendix A - Supported Databases

- MS SQL Server
- PostgreSQL
- MySQL / MariaDB
- Oracle

Appendix B - Legacy/Deprecated Databases

- IBM DB2
- ADABAS

Number: POL0020026
Revision Number: 2
Revision Date: 2017-12-19
Effective Date: 2004-03-09
Last Reviewed: 2024-09-13

DDoS Standard

Purpose

This standard exists to provide guidance on the enterprise standards for [distributed] denial of service attacks and mitigations.

Principles:

- DDoS attacks are broken into 3 different classifications, through the use of layers of technology, NDIT provides coverage for all attack methods. Although protections are in place, due to the nature of DDoS, it is impossible to guarantee coverage. There will always be attacks that can impact services.

Standard

Volumetric based attacks:

Volumetric attacks are simply attacks that flood a physical internet link with traffic. Source addresses are spoofed, and blocking source addresses has no impact. This class of attacks can not be mitigated within STAGEnet and must be done upstream

1. DCN is the current internet provider in Bismarck. DCN, as part of the Internet contract, provides DDoS protection and scrubbing via dedicated appliances.
2. Midco is the current internet provider in Fargo. Midco, as part of the Internet contract, provides DDoS protection and scrubbing via dedicated appliances.

Session based attacks

Session based attacks are designed to exhaust available sessions available in a stateful device, which may be a firewall, load balancer, or server. Blocking source addresses may not be useful, as spoofed half-open TCP sessions can be part of this attack. This attack can be accomplished with a low to medium volume of traffic.

1. NDIT protects from session based attacks with 2 methods:
    1. Zone protection policies on the Palo Alto NGFW's provide common protocol based session attacks
    2. Firewall based DDoS policies protected limited IP ranges (Proxy/F5) within the datacenter.
    3. NDIT has started to deploy a cloud based WAF for selected websites which also offers protection from this type of attack.

Resource based attacks

Resource based attacks are designed to overload a server with valid but extremely time consuming requests. Often, the web server may query a database with a slow running query, and the attacker will launch as many of these concurrent attacks as possible. Very little network traffic is required, and often is less than normal day-to-day averages. Because a full TCP session must be established, IP blocking is effective but may be problematic if the attack is very distributed.

Resource based attacks are both difficult to prevent as well as difficult to remediate.

1. During an attack, adding additional hardware may help mitigate the attack.
2. Software fixes to the application are the preferred fix to close the attack vector entirely.
3. NDIT has started to deploy a cloud based WAF for selected websites which also offers protection from this type of attack.

Scope

The standard applies to all STAGEnet traffic.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

```
Number: POL0030001
Revision Number: 1
Revision Date: 2024-09-16
Effective Date: 2024-09-16
Last Reviewed: 2024-09-16
```

Digital Asset Management Standard

Purpose

Standardize the solution to provide the enterprise with the ability to manage digital assets.

Standard

1. AssetBank from Bright Interactive; will be used to fulfill digital asset management business needs.

Definitions

Digital Asset Management - Digital asset management is an effective solution to store, organize, find, retrieve and share digital content from a central location. It provides stakeholders controlled access to digital assets, including images, photos, creative files, video, audio, presentations, documents, and more.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020170
Revision Number: 1
Revision Date: 2021-04-05
Effective Date: 2021-04-05
Last Reviewed: 2024-09-13
```

Document Management Solution Standard

Purpose

Standardize the solution(s) to provide the enterprise with the ability to manage electronic document with a document management solution.

Standard

1. Microsoft SharePoint
2. FileNet

Definitions

Document Management - Document management is a system used for document storage and organization, version control, access controls and permissions, collaboration, search capabilities, workflow and automation capabilities, integration with other products, and to help with compliance and governance.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020183
Revision Number: 2
Revision Date: 2024-12-20
Effective Date: 2021-04-07
Last Reviewed: 2024-12-20
```

Domain Name Standard

Purpose

Align the state with the official government domain (.gov). This will ensure that domain names are under the administration of the state, reducing the possibility of undesirable domains being misconstrued as official government sites. Instill public trust in government websites through the use of the .gov domain.

Standard

1. The official North Dakota government domain is **nd.gov**.
2. All public facing domains shall be registered as at least a fourth-level domain within the nd.gov domain. The third level shall uniquely identify the state agency or service. Example domain name: ***service.agency.nd.gov***
3. Internal domains must uniquely identify the state agency or service and shall not use generic or public facing branding terms.
4. All registered nd.gov domains shall adhere to all federal .gov domain registration requirements and guidelines.

Definitions

Domain Level - Refers to the hierarchical position of a specific segment within a domain name. Domain levels start from right to left, starting with the top-level domain.

Example: In the domain ***service.agency.nd.gov***:
- ***gov*** is the top-level domain
- ***nd*** is the second-level domain
- ***agency*** is the third-level domain
- ***service*** is the fourth-level domain

Domain Name - A domain name is a user friendly way of finding and identifying computers on the Internet.

Internal Domains - Domains only accessible from STAGEnet and not available from the public internet.

STAGEnet - (Statewide Technology Access for Government and Education network) utilized by all state and local government and K12.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020019
Revision Number: 6
Revision Date: 2025-06-02
Effective Date: 2005-07-18

Last Reviewed: 2025-06-02

E-Services Privacy Standard

Purpose

Privacy issues are of concern for many people who are asked to provide personal information through e-services. Privacy standards may ease the concern of the customer and hopefully encourage the use of the services.

Standard

1. All e-services accepting personally identifiable information shall provide privacy policy information.
   Privacy policies shall state:

   1. What and why personally identifiable information is collected.
   2. How the information will be used and under what circumstances it will be released, or if applicable the specific laws providing that the information is confidential.
   3. Choices available to the individual for reviewing and correcting customer submitted information.
   4. Contact information.
   5. If social security numbers are collected, notification as required in the Privacy Act of 1974 must be given.
   6. Reference to a security policy.
   7. The web pages/applications or specific type of information/service areas covered by this policy.
   8. If and how cookies are used.

Definition

Personally identifiable information - Any recorded information that uniquely identifies the person, such as, but not limited to, name, account number, social security number, user ID, PIN number, e-mail address, or biometric data. Data that can be tied to a device or residence owned or used by an individual, such as, but not limited to, the individual's telephone number, mailing address or computer IP address.

E-Services - Services provided electronically via interactive media. For example but not limited to:

- Interactive Voice Response (IVR)
- World Wide Web

Cookies - Cookies are text files that are transmitted between your browser and the web server. There are two types of cookies:

- In memory cookies - deleted on closing browser
- Disk cookies are stored until they expire or are deleted.

Guidance

1. E-Services Privacy Policy Best Practices
2. Sample Privacy Policy and Disclaimer
3. Privacy Act of 1974
4. Guidelines from the Online Privacy Alliance

Policy

Inform customers of the agencies' intentions regarding the privacy of their personal information.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020129
Revision Number: 2
Revision Date: 2004-11-02
Effective Date: 2004-03-14
Last Reviewed: 2024-09-13

E-Services Security Standard

Purpose

Ensure agencies that engage in online activities or electronic commerce use due diligence to protect customer information from misuse or unauthorized access.

Standard

1. Agencies requesting customer information shall provide a secure method for collection in compliance with the Encryption Standard.
2. Credit card numbers collected via e-services will not be stored electronically.
3. Credit card transactions shall be processed securely and must use Bank of North Dakota (BND) approved vendors.

Definition

Customer information - Any recorded information that identifies the person, such as but not limited to: account number, social security number, user ID/ PIN number/password, driver's license number. Other information to be considered based on agency business, such as but not limited to: name, mailing address, e-mail address.

E-Services - Services provided electronically via media that is interactive. For example but not limited to:

- Interactive Voice Response (IVR)
- World Wide Web

Customer - Any entity doing business with the state of ND on their own or another's behalf.

Guidance

1. Encryption Standard

Policy

Ensure customer information is handled securely.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020118
Revision Number: 2
Revision Date: 2017-06-27

Effective Date: 2005-07-18
Last Reviewed: 2024-09-13

Electronic Data Backup Standard

Purpose

To guarantee backup copies of data are created so that data availability and retention objectives are satisfied.

Standard

1. Agencies must review their data and identify backup requirements.
2. Backup procedures, frequencies and retention are defined, documented and must adhere to Continuum of Government guidelines.
3. At the completion of each scheduled backup, logs must be checked and verified to ensure successful data backup has occurred.
4. Offsite storage of backup media is required.
5. Backups must be tested periodically to validate recoverability.

Definition

Backup Procedures - Documented procedures that identify the backup process.

Policy

Each agency or designated custodian ensures backup of data on a regular basis to minimize data loss.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Guidance

1. State and Federal record retention schedules.
2. Continuum of Government Guidelines.

```
Number: POL0020224
Revision Number: 1
Revision Date: 2004-07-05
Effective Date: 2004-07-05
Last Reviewed: 2024-09-13
```

Electronic Signature Standard

Purpose

Standardize on the use of Adobe Sign as the preferred Electronic Signature solution.

Standard

1. Adobe Sign will be used to fulfill Electronic Signature business needs.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020058
Revision Number: 1
Revision Date: 2021-04-01
Effective Date: 2021-04-01
Last Reviewed: 2024-09-13

Email Standard

Purpose

1. To utilize feature-rich functionality beyond basic industry standards and achieve 100% integration and interoperability throughout the enterprise.
2. To create systems of nominal complexity so that support and administrative efforts can be minimized, training can be leveraged, and job duties can be refocused to reduce redundancy.
3. To allow for rapid deployment of new technology and position the enterprise to react quickly to emerging opportunities, problems, and threats.
4. To simplify the end-user's experience.
5. To utilize a single directory for authentication, access control, directory lookups, and distribution lists.
6. To project a consistent view of state government to the public.
7. To avoid duplication of system resources and leverage enterprise licensing.

Standard

1. All Email functionality will be provided using enterprise solutions specified in Appendix A.
2. All agencies shall use and publish a single, enterprise-wide email domain of "@nd.gov".
3. All agencies shall maintain a generic agency email address (an "Info" account).
4. All agencies shall maintain an email distribution group that contains all email users within their agency, and that group shall be configured to accept messages from a group of "Authorized Senders To All."
5. User-IDs and email addresses shall be named in accordance with the EA Security Architecture "Access Control" standard.
6. All email from the public must pass through enterprise email gateways.

Definition

Email (electronic mail) - A means of transmitting computer-based messages over a network, typically the Internet. Today's email programs are often bundled with other tools designed to improve collaboration, such as calendars, contact lists, and task lists.

Policy

A standardized set of technologies will be used across the enterprise for Email functionality.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

APPENDIX A

Email System Components

Email

- Microsoft Exchange
- POP3/SMTP service

Number: POL0020033
Revision Number: 3
Revision Date: 2018-10-10
Effective Date: 2013-08-13
Last Reviewed: 2024-09-13

Employee Security Awareness Standard

Purpose

To establish an employee security awareness policy which will ensure employees that utilize the state network are informed of current security best practices recommended for technologies being utilized by the state.

Standard

1. Employees shall complete the NDIT provided Information Security Awareness overview on their first day of employment.
2. Employees shall complete the NDIT Information Security Awareness Training within the first three business days of being given credentials to access the state government network.
3. Employees shall complete the NDIT Information Security Awareness Training (Refresher) annually.
4. Employees shall complete the ongoing Information Security Awareness Trainings quarterly.
5. Employees that do not complete trainings within sixty (60) days of being assigned will be reported to their agency's HR Division
6. Social Engineering Campaign Trainings:
    1. All failed phishing campaigns will receive the Social Engineering Indicator page as their training.
    2. Employees failing three (3) campaigns during a twelve (12) month period will be required to take an additional training.
    3. Employees failing four (4) campaigns during a twelve (12) month period will be required to attend a cybersecurity training presented by NDIT. The employee's supervisor will be notified.
    4. Employees failing five (5) or more campaigns during a twelve (12) month period will result in NDIT Security contacting the agency's HR Department.

Definition

Employee - This includes state government employees and non-state government employees. Non-state government employees are individuals employed by a private vendor and are working on a state project.

State Government Network - "Internal", is used to outline the perimeter of the network infrastructure used solely for State Agencies and excludes other government branches, such as, K12, North Dakota universities, and other political sub-divisions attached externally to the State network.

Social Engineering - Broad range of malicious activities performed through human interactions by using psychological manipulation to deceive users into making security mistakes or giving away sensitive information. Common forms include: phishing (email), vishing (voice), and smishing (text message).

Policy

To provide security awareness to enhance the protection of the state information technology infrastructure.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020119
Revision Number: 5
Revision Date: 2022-10-24
Effective Date: 2005-07-19
Last Reviewed: 2024-09-13

Encryption Standard

Purpose

To ensure that the disclosure of sensitive information to unintended recipients has been minimized.

Standard

1. Encryption shall be used when the electronic transmission of information involves sensitive data that passes over the public network.
2. All portable computers containing sensitive data shall employ full-disk encryption.
3. Sensitivity of data will be determined by the government entity administering the data or the application.
4. All remote access shall require encrypted communications. This is addressed by the standard ST002-04.1 Remote Access standard.
5. If data encryption is used, the government entity administering the data or the application shall have a recovery plan for encryption keys.
6. All logons that pass over the public network shall utilize an encrypted process.

Definition

Sensitive information - Confidential information as defined in North Dakota Century Code and federal regulations as well as information that has been designated as needing additional safeguards. Examples of sensitive information are social security numbers, home telephone numbers, home addresses, user IDs/passwords.

Public Network (External) - Any network infrastructure not managed by ITD and not used for the purpose of the State Government network.

Portable Computer - Laptops, Tablet PCs, and Netbooks.

Guidance

For internal hosts that have capability of using encrypted logons, it is recommended that this be used.

Policy

To provide a common encryption practice to protect sensitive information.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020120
Revision Number: 2
Revision Date: 2011-09-12

Effective Date: 2005-07-18
Last Reviewed: 2024-09-13

Endpoint Security Protection Standard

Purpose

Minimize risk of malicious attacks or via malicious software and identify vulnerabilities by implementing minimum operating standards as it relates to endpoint security software.

Standard

1. The State's approved and centrally managed anti-malware and vulnerability solutions shall be installed and active on all State-managed devices.
2. Endpoint security software and associated signatures shall be configured to automatically update when new releases become available.
3. All incoming files will be scanned in real-time for malware.
4. Vulnerability scans will be performed daily on workstations and weekly on servers.
5. Files containing malware will be prevented from executing or will be deleted.
6. Email shall be scanned in real time for malicious content through the State’s approved email solution.
7. State-issued mobile devices shall have the State’s approved mobile device management software installed for devices that can effectively run the client.
8. State’s approved mobile device management software shall implement additional security protections for non-state devices authorized to access state data.

Definition

Mobile Device - A mobile device is a handheld device with local storage, cameras and video recording capability which includes but is not exclusive to smart phones, smart watches and tablets. Mobile devices support the synchronization of local data with a different location such as a laptop, server or automated cloud backup.

Endpoint - Any physical system that connects to and exchanges information with a computer network (e.g. server, workstation, laptop).

Malware - malicious software, trojans, ransomware, backdoors, rootkits, viruses, and spyware.

Vulnerability - a flaw in code or design that creates security risk of an endpoint

Signature - The binary pattern of malware, used by the anti-malware program to detect and eliminate the malware.

Guidance

The intent is to have security protection on all devices that have the potential of malware exploitation.

Policy

Implement and maintain enterprise security protection solutions on state devices.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Governance and Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Noncompliance to this standard has been classified as high-risk i.e. having impact on the integrity of enterprise information systems. Violations to this standard will result in NDIT operations taking immediate action to prevent enterprise risk prior to the reporting of noncompliance to the Office of the State Auditor.

Number: POL0020186
Revision Number: 7
Revision Date: 2024-07-31
Effective Date: 2004-03-15
Last Reviewed: 2024-07-31

Enterprise Database Security Standard

Purpose

Prevent unauthorized access to data in databases and achieve efficiencies in database consolidation. Adherence to this standard will ensure data consistency, proper management of disaster recovery, backups, point in time recovery processes and application testing.

Standard

1. Every database will have at least three distinct areas: development, acceptance testing and production.
   Administrative privileges on production and acceptance testing database areas:

   - **Multi-agency shared infrastructure** will be restricted to the agency hosting the database.
   - **Single agency infrastructure** will be restricted to the either the agency hosting the database or the agency's DBA staff.
3. Migrating changes from acceptance test to production requires that the agency who owns the data have a formal acceptance testing and sign off process.
4. Agency assigned developers will have developer privileges to development database areas.
5. Create user privileges on all database areas will be restricted to the database or security administrators.
6. Access to system level views of database catalog information will be restricted.
7. Migrating changes from development to acceptance test is requested by the agency assigned developers.
8. Database scripts which modify database objects will be reviewed, approved, and run on production and acceptance test databases by the database administrators.
9. Installation and creation of production, acceptance test and development databases for new systems must be performed by the database administrators.
10. User authentication shall utilize the enterprise Microsoft Active Directory if supported by the Database.
11. Personnel administering vendor applications that control changes to database objects through the vendor's tool and not scripts will be allowed to apply upgrades to all database areas. Prior to deployment in production, the changes created by the tool must be reviewed to assure that all changes adhere to this standard. In addition, before any changes are made to any database area, backups must be taken for recovery purposes.

Definition

Administrative Privileges:

Administrative privileges include the administration of a database, database objects and users. These privileges are explained in the following categories:

- Privileges to perform system wide actions that affect the whole database, which in turn can affect recoverability and performance. These privileges allow the administration of database objects such as tablespaces, rollback segments, and control files. They allow users to change database parameters and restrict a database or terminate user sessions.
- Privileges to modify all database objects defined in the database, which may be for multiple agencies and/or multiple applications. These privileges are ones that include the keyword "ANY" which allows access to all objects in a database regardless of who owns them, such as "DROP ANY TABLE".
- Privileges to access all the data and code in a database, which can be for multiple agencies and/or multiple applications. For example using the keyword ANY (SELECT ANY TABLE).
- Privileges to setup database security. For example allowing the creation of users (end users and table owners) in a database, granting object privileges, creating and granting roles, creating profiles, and granting the ability to grant security to another user via the keywords "WITH ADMIN OPTION" and "WITH GRANT OPTION".

Developer Privileges:

Developer privileges include the modification of a specific set of database objects. For example using the commands ALTER, CREATE, and DROP of database objects such as tables, functions, procedures, triggers, views, and roles.

Guidance

1. Database Security Best Practices

Policy

Administrative privileges are not freely given to applications or non-administrative personnel.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020121
Revision Number: 1
Revision Date: 2006-05-15
Effective Date: 2006-05-15
Last Reviewed: 2024-09-13
```

Enterprise WiFi Standard

Purpose

Aruba has been chosen as our enterprise WiFi vendor.

Standard

1. NDIT utilizes a single vendor solution for all WiFi deployments, managed through a centralized deployment and procured through the STAGEnet equipment RFP & Contract
2. Approved Vendor(s):
   - HPe Aruba

Scope

This standard applies to all State government entities utilizing STAGEnet.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020060
Revision Number: 1
Revision Date: 2021-04-01
Effective Date: 2021-04-01
Last Reviewed: 2024-09-13

File Management, State Employee Standard

Purpose

Standardize the solution to provide the enterprise with the ability to store, share and manage state employee data files.

Standard

1. OneDrive as part of M365 Provided by Microsoft; will be used to fulfill personal file management.

Definitions

Personal File Management - Personal file management has limited capabilities and is designed to manage individual or group files.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020195
Revision Number: 3
Revision Date: 2025-02-26
Effective Date: 2021-05-13
Last Reviewed: 2025-02-26

File Transfer, System Integration Standard

Purpose

Standardize the solution to provide a solution to manage the transferring of digital files across the enterprise.

Standard

1. MOVEit by Ipswitch; will be used to fulfill the system integration file transfer business needs.

Definitions

System Integration File Transfer - System integration file transfer is a technology platform that allows organizations to reliably exchange electronic file-based data between systems in a secure way to meet compliance needs.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020196
Revision Number: 2
Revision Date: 2025-02-26
Effective Date: 2021-05-13
Last Reviewed: 2025-02-26

Fixed Asset Management, Large Standard

Purpose

Standardize the solution to provide the enterprise with the ability to manage large fixed assets.

Standard

1. PeopleSoft Financials and Supply Chain Management (FSCM) from Oracle will be used for fixed asset management for assets valued $10,000 or more.

Definitions

Fixed Asset - Fixed asset inventories include eight distinct classes: Equipment, Construction-in-Progress, Buildings and Building Improvements, Infrastructure, Land, Land Improvements, Lease, and Subscription Based IT Arrangements (SBITA). *Refer to "OMB Fiscal & Administration Policies" appendix A for further description.*

Guidance

- Fiscal and Administrative Policy - Policy 205 – Fixed Assets
- Fiscal and Administrative Policy - Appendix A - Fixed Asset Accounting Policies

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020185
Revision Number: 2
Revision Date: 2025-05-02
Effective Date: 2021-04-08
Last Reviewed: 2025-05-02
```

General Ledger Standard

Purpose

Standardize the solution to provide the enterprise with the ability to manage general ledger.

Standard

1. PeopleSoft Financials and Supply Chain Management (FSCM) from Oracle; will be used to fulfill general ledger business needs.

Definitions

General Ledger - A general ledger represents the record-keeping system for a company's financial data with debit and credit account records. The general ledger provides a record of each financial transaction that takes place.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020174
Revision Number: 1
Revision Date: 2021-04-06
Effective Date: 2021-04-06
Last Reviewed: 2024-09-13
```

Geographic Information Systems Standard

Purpose

Standardize the solution to provide the enterprise with the ability to manage geographic information.

Standard

1. ArcGIS provided by Esri will be used as Geographic Information Systems.

Definitions

Geographic Information System - A geographic information systems is used for creating and using maps, compiling geographic data, analyzing mapped information, sharing and discovering geographic information, using maps and geographic information in a range of applications, and managing geographic information in a database.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020184
Revision Number: 1
Revision Date: 2021-04-07
Effective Date: 2021-04-07
Last Reviewed: 2024-09-13

Grant Management Standard

Purpose

Standardize the solution to provide the enterprise with the ability to manage grants.

Standard

1. WebGrants from Dulles Technologies Partners; will be used to fulfill grant management business needs.

Definitions

Grant - Grants are non-repayable funds or products disbursed or given by one party (grant makers) to a recipient.

Grant management **-** Grant management solutions help grant makers administer the grant process. This includes activities such as organize, prioritize, and process the grant applications they receive from recipients.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020156
Revision Number: 1
Revision Date: 2021-04-01
Effective Date: 2021-04-01
Last Reviewed: 2024-09-13

Imaging Standard

Purpose

To share knowledge and data, coordinate training, promote user groups and reduce cost of training and purchase of tools.

Standard

1. All new Enterprise Image Capture Systems shall use the tools as identified in Appendix A.
2. If a record has a permanent retention, then the minimum dpi shall be 300 dpi, else 200 dpi shall be the minimum.
   Standard Image Formats include:

   - .tiff (G3 & G4) - Tagged Image File Format, Tag Image File Format
   - multi-page .tiff - Tagged Image File Format, Tag Image File Format
   - .xml - Extensible Markup Language
   - .pdf - Portable Document Format
   - .pdf/a - Portable Document Format Archive
   - .jpg, .jpeg - Joint Photographic Experts Group
   - .png - Portable Network Graphics
   - .bmp - Bitmap Image File
   - .gif - Graphics Interchange File
4. Documented procedures shall be in place for imaging documents to prove document trustworthiness per Federal and State Rules of Evidence and other applicable regulations.

Definition

Capture System - A system for automated scanning or processing of documents. Includes scanning, indexing, quality assurance, and storage.

Imaging - Process of creating an electronic picture of a document using a scanner or electronic process.

Enterprise Image Capture System - A Capture System used to satisfy the needs of an organization rather than individual users.

Policy

Tools will be consistent throughout the enterprise.

Applicability

All documents defined as a record per N.D.C.C. 54-46-02.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Appendix A

Tools

- Ilinx
- Ilinx Email Import
- HP Teleform Mediclaim
- Open Scan - Mail Scan

Number: POL0020028
Revision Number: 2
Revision Date: 2017-06-01
Effective Date: 2004-05-11
Last Reviewed: 2024-09-13

Incident, Prevention, Response, and Notification Standard

Purpose

To communicate any vulnerabilities or incidents to the necessary individuals.

Standard

1. ITD shall designate an individual to coordinate the incident prevention/response/notification process.
2. The ITD coordinator shall communicate any incidents or vulnerabilities they become aware of to agency contacts.
3. Each state agency (or customer of ND IT) shall designate an agency contact.
4. The agency contact shall communicate any incidents or vulnerabilities they become aware of to appropriate agency personnel.
5. The agency contact shall, in a timely manner, correct any vulnerabilities or incidents they become aware of and report such activities.

Definition

Contact - This individual is expected to be filling the IT Security Officer role for the agency.

Policy

To provide a coordinated enterprise communication process to address incident prevention/response/notification.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020122
Revision Number: 1
Revision Date: 2004-05-11
Effective Date: 2004-05-11
Last Reviewed: 2024-09-13
```

Information Technology Procurement Standard

Purpose

This standard provides agencies with the process to follow for the procurement of Information Technology (IT) hardware, software, and services. Technology procurements are reviewed prior to the actual purchase transaction to ensure compliance with IT standards, consistency with enterprise architecture, conformance to agency IT plans, assessment of third-party risks, and adherence to procurement best practices.

Standard

1. NDIT adopts OMB Central Services Division (CSD) purchasing procedures as defined in the State Procurement Manual as a standard for all technology purchases.
2. **IT Review:** The originating agency shall be responsible to initiate an IT Review of its IT purchases, competitive bid solicitations, and contracts that exceed the purchase approval limits for the categories below.

   Purchase Approval Limits: Approval limits for IT procurement are categorized below. NDIT approval is required for purchases or contracts according to the limits below.

Limits	Category	Definition
$0 and over	Application and Data Services	Includes all applications and data services not directly managed or hosted by NDIT, including all Software-As-A-Service (SaaS) and cloud solutions.
	IT Server and Network Services (Data, Voice, Video) Equipment	Includes any, but not limited to, server equipment that provides functions such as applications, electronic mail, file and print, database, and server storage.
Level 2 and above	Other IT Equipment	Includes any type of information technology hardware and supporting infrastructure not covered by an above category.
	Professional Services	Professional services contracts for design, development, and related activities for implementation of information technology applications or systems, which may include both hardware and software components and ongoing maintenance/support. Note: All open-ended or hourly IT contracts without a guaranteed maximum payment or 'not to exceed' amount must be reviewed by NDIT.

Level 2 and above - Solicitations, Alternate Procurements, and Contract Review: For solicitations, including invitations for bids (IFB) and requests for proposals (RFP), alternate procurement (AP) requests, and contracts where the anticipated procurement is Level 2 and above, the agency shall submit an IT Review prior to issuing the appropriate procurement.

1. A copy of the solicitation, contract, or alternate procurement purchase request must be attached to the IT Review.
2. If not previously requested by the originating agency, the technology specifications for the procurement may be attached to the IT Review.
3. Approval must be obtained from NDIT before issuing the purchase order or signing the contract.

Policy

54-59-05 Information Technology Department - Powers and duties.

Each executive branch agency or institution, excluding the institutions under the control of the board of higher education, shall submit to the department, in accordance with guidelines established by the department, a written request for the lease, purchase, or other contractual acquisition of information technology. The department shall review requests for conformance with the requesting entity's information technology plan and compliance with statewide policies and standards. If the request is not in conformance or compliance, the department may disapprove the request or require justification for the departure from the plan or statewide policy or standard.

Applicability

This standard applies to all executive branch state agencies and institutions, excluding the institutions under the control of the board of higher education.

Definition

Information Technology - Citing ND Century Code (Chapter 54-59-01.3), "'Information technology' means the use of hardware, software, services, and supporting infrastructure to manage and deliver information using voice, data, and video." NDIT further defined this in its Definition of Information Technology.

State Term Contracts - The State Procurement Office has established term contracts for commodities commonly used by the state. Term contracts establish a supplier for specific commodities for a fixed period of time. Examples are term contracts for desktop computer equipment and printer equipment.

Invitation for Bid (IFB) - The Invitation for Bid (IFB), solicitation is used to request competitive sealed responses. The document includes or incorporates by reference a description of the needed commodity, specifications or scope of work, bidders' instructions, contractual terms and conditions, evaluation criteria, price sheets for vendors to submit prices, and offer and acceptance sheet.

Request for Proposal (RFP) - The Request for Proposal (RFP) solicitation is used to request competitive sealed responses when award will be based on factors in addition to price, and when it is expected that any aspect of the requirements will need to be negotiated with respondents as part of the selection process and contract award.

Alternate Procurement (AP) - The Alternate Procurement (AP) request is used when a non-competitive procurement, limited competitive procurement, or purchase from another government entity's contract is sought.

Guidance

- Procurement Laws, Rules, Guidelines

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor and non-compliance to this standard represents a violation of state law. This standard communicates guidance for actions to be taken by agencies to remain in compliance.

Number: POL0020208
Revision Number: 2
Revision Date: 2023-08-08
Effective Date: 2004-01-11
Last Reviewed: 2024-09-13

Interactive Voice Response (IVR) Standard

Purpose

Standardize the solution to provide the enterprise the ability to provide interactive voice response systems.

Standard

1. Genesys Cloud IVR will be used to fulfill the IVR business needs.

Definitions

Interactive Voice Response (IVR) - Interactive voice response is a technology that allows humans to interact with a computer-operated phone system through the use of voice and DTMF tones input via a keypad.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020204
Revision Number: 2
Revision Date: 2025-01-09
Effective Date: 2021-06-04
Last Reviewed: 2025-01-09

IT Service Management Standard

Purpose

Standardize the solution to provide the enterprise with IT service management capabilities.

Standard

1. IT Service Management from ServiceNow; will be used to fulfill IT service management needs.

Definitions

Incident Management - Activities to identify, analyze, and restore normal service operation.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020192
Revision Number: 2
Revision Date: 2025-02-26
Effective Date: 2021-05-12
Last Reviewed: 2025-02-26
```

IT Services Standard

Purpose

Utilize IT Services provided by and managed by NDIT as mandated in North Dakota Century Code (Chapter 54-59-22).

Standard

1. The following IT services must be provide by NDIT:
    1. Electronic Mail
    2. File-and-Print Server Administration
    3. Database Administration
    4. Storage
    5. Application Servers
    6. Hosting Services

Scope

This standard applies to each state agency and institution, excluding the legislative and judicial branches, the institutions under the control of the state board of higher education, the attorney general, the veterans' home.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020024
Revision Number: 1
Revision Date: 2021-07-07
Effective Date: 2021-07-07
Last Reviewed: 2024-09-13

Layer 2 IP Network Switching Standard

Purpose

Extreme Networks has been chosen as our enterprise L2 vendor.

Standard

1. NDIT utilizes a single vendor solution for all L2 deployments, managed through a standardized template deployment and procured through the STAGEnet equipment RFP & Contract

   Approved Vendor(s):

   - Extreme Networks

Scope

This standard applies to all State government entities utilizing STAGEnet.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020015
Revision Number: 1
Revision Date: 2021-04-01
Effective Date: 2021-04-01
Last Reviewed: 2024-09-13
```

Layer 3 Addressing Standard

Purpose

To address and organize both the private internal ip addressing and public addressing. This includes both IPv4 and IPv6.

Standard

1. NDIT utilizes a single centralized management of ip address deployments, managed through a standardized template deployment where possible.
2. Approved Vendor(s):
   - Infoblox - DNS/DHCP/IPAM
   - All other solutions needs architecture approval.

Scope

This standard applies to all STAGEnet entities, excluding all higher education institutions, i.e. campuses and agricultural and research centers, and veterans home.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020016
Revision Number: 1
Revision Date: 2021-04-01
Effective Date: 2021-04-01
Last Reviewed: 2024-09-13
```

Layer 3 NAT Networking Standard

Purpose

To address and organize both the private internal ip addressing and public addressing.

To enable internal private ip space access to external resources and external ip space to internal private resources.

Standard

1. All NAT'ing within STAGEnet private 10.0.0.0/8 space must be performed by NDIT, per the specifications of the NAT standard. Individual entities are NOT permitted to NAT within STAGEnet, as it may break numerous components and design elements. All endpoints within STAGEnet are to utilize private IPv4 addresses. Endpoints requiring connectivity originating from public IP space require NAT'ing at the network layer.
2. NAT'ing may be required for connectivity to vendors. NAT for this use-case should reside on the terminating STAGEnet IPSEC device.
3. All Data Center NAT'ing will centrally take place within the Data center external/internet facing boundary appliance/firewall.
4. All other NAT'ing will centrally take place on the the Stagenet external/internet facing boundary appliance/firewall.
5. All NAT'ing address will be entered into the centralized IPAM solution.
6. Approved Vendor(s):
   - Infoblox - DNS/DHCP/IPAM
   - Palo Alto Networks - L7 Firewall
   - Juniper Networks - L3/4 Firewall (SRX)

Scope

This standard applies to all STAGEnet entities, excluding all higher education institutions, i.e. campuses and agricultural and research centers, and veterans home.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020017
Revision Number: 1
Revision Date: 2021-04-01
Effective Date: 2021-04-01
Last Reviewed: 2024-09-13
```

Low-Code / No-Code Application Platform Standard

Purpose

Standardize the solution(s) to provide low-code/no-code application platform capabilities within the enterprise to streamline and unify the approach to application development. This standardization aims to:

- **Reduce Complexity:** Limiting the number of platforms in use reduces the complexity of the technology environment, making it easier to manage, support, and secure.
- **Enhance Productivity:** With standard platforms, employees can quickly learn and become proficient in application development, leading to faster delivery of solutions and a more agile response to business needs.
- **Improve Collaboration:** A common set of tools can improve collaboration between business and IT teams, as they can work together using a shared language and set of capabilities.
- **Control Costs:** Standardization can lead to cost savings through volume licensing agreements and reduced training and support costs.
- **Ensure Compliance:** With fewer platforms to govern, less effort is needed to enforce compliance with security, data protection, and other regulatory requirements.
- **Accelerate Integration:** Standard platforms are more likely to offer pre-built integrations with other enterprise systems, simplifying the process of connecting applications and data.
- **Increase Reusability:** Foster an environment where components, workflows, and templates can be reused across different applications to reduce redundant work and maintain a high level of quality and consistency.
- **Promote Innovation:** These platforms can empower business users to create solutions themselves, fostering a culture of innovation and allowing IT to focus on more complex tasks.

Standard

1. Approved Low-Code / No-Code Application Platform(s):
    1. Microsoft Power Platform
    2. ServiceNow Platform
2. STATE managed platform instances will be used for all test and production application deployments

Definitions

Low-Code/No-Code Application Platform - Software environments that enable the creation of applications through graphical user interfaces and configuration instead of traditional computer programming. Low-code platforms may require some coding to extend functionality, while no-code platforms are designed to operate without writing any code at all, making application development accessible to non-technical users.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020264
Revision Number: 1
Revision Date: 2024-04-18
Effective Date: 2024-04-18
Last Reviewed: 2024-09-13

Mobile Application Publishing Standard

Purpose

Align the state with the official government publisher. This will ensure that applications are under the administration of the state, reducing the possibility of undesirable applications being misconstrued as official government applications.

Standard

1. Mobile applications published to the Apple and/or Google application stores for distribution will use the existing "**State of North Dakota**" publisher.

Definitions

Application Store - Mobile application marketplaces - Apple App Store and Google Play Store

Mobile Application - An application specifically targeted to run natively on phone and tablet devices.

Publisher - Common parent account that child applications are associated under.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020253
Revision Number: 1
Revision Date: 2023-05-05
Effective Date: 2023-05-05
Last Reviewed: 2024-09-13
```

Mobile Device Access Control Standard

Purpose

To establish security procedures for access to mobile devices thereby ensuring the reliability, accessibility, and security of such devices and the state network.

Standard

REDACTED - Contact NDIT for more information

Number: POL0020123
Revision Number: 8
Revision Date: 2025-01-06
Effective Date: 2007-11-14
Last Reviewed: 2025-01-06

Office Productivity Suite Standard

Purpose

Standardize the solution to provide the enterprise with the suite of products to provide information.

Standard

1. Office 365 from Microsoft; will be used to fulfill the needs for an office productivity suite of tools.

Definitions

Office Productivity Suite - A Office Productivity Suite is a bundle of productivity software intended to be used by office workers. The components are generally distributed together, have a consistent user interface and usually can interact with each other.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020193
Revision Number: 1
Revision Date: 2021-05-12
Effective Date: 2021-05-12
Last Reviewed: 2024-09-13

Operating System Standard

Purpose

To provide a secure, stable, and supported operating system on all Network Connected Devices (NCDs) within the Enterprise.

Standard

1. All NCD operating systems within the enterprise will support directory authentication as defined by EA Security standard SS005.2.
2. All NCD operating systems will adhere to enterprise anti-virus requirements as defined by EA Security standard SS001.4.
3. All NCD operating systems deployed in the enterprise shall be actively supported with patches and updates pertaining to the OS.
4. All critical updates will be installed within 14 days of the release date on all NCDs.

Definition

Network Connected Devices (NCD) - A device on a network that provides computing resources to one or more end users. Devices include but are not limited to tablets, laptops, desktops, workstations, printers, multi-function printers, and mobile devices.

Active Support - Active support is considered to be support that addresses relevant security vulnerabilities that are identified within the OS. The entity providing the OS support shall maintain a concerted effort to address all security issues with patches and upgrades through an appropriate documented management process.

Critical Updates - Any updates, excluding service packs or general OS updates, which the OS vendor defines as critical or security related.

Policy

NCD operating systems will provide a secure, stable, and supported platform.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020130
Revision Number: 1
Revision Date: 2016-06-22
Effective Date: 2016-06-22
Last Reviewed: 2020-03-05
```

Payroll Standard

Purpose

Standardize the solution to provide the enterprise with the ability to provide HR Payroll Management.

Standard

1. PeopleSoft Human Capital Management Suite from Oracle; will be used to fulfill HR Payroll business needs.

Definitions

Payroll ***-*** *List of employees entitled to payments, other work benefits, and the amounts that each should receive, as well as records of previous payments, bonuses, and taxes.*

PeopleSoft Human Capital Management Suite - *PeopleSoft Payroll provides all the tools need to run an efficient payroll operation. Basic information about the types of balances that you want to maintain, how you want to group the workforce and when you want to pay them. In addition, you can define and establish earnings, deductions, and taxes, to fit your unique business needs and manage employee-level data.*

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020180
Revision Number: 1
Revision Date: 2022-10-05
Effective Date: 2022-10-05
Last Reviewed: 2024-09-13

Physical Access Standard

Purpose

To establish a physical security policy which will ensure servers and workstations are protected and to minimize the risk of unauthorized access to the state government network.

Standard

1. All servers shall be located in an area of minimal traffic and physical access to the servers shall be restricted to authorized personnel. All visitors shall be logged in and escorted by an authorized person.
2. All servers and workstations shall require logons. Local guest and anonymous accounts shall be deactivated or deleted. Servers and Workstations shall be either manually logged off or locked prior to leaving them unattended.
3. All workstations shall have automatic screen locking active with a maximum of a 15-minute activation time.

Definition

State Government Network (Internal) - Used to outline the perimeter of the network infrastructure used solely for State Agencies and excludes other government branches, such as, K12, North Dakota universities, and other political sub-divisions attached externally to the State network.

Policy

To protect the state information technology infrastructure from unauthorized physical access.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020124
Revision Number: 2
Revision Date: 2017-06-27
Effective Date: 2005-07-18
Last Reviewed: 2024-09-13

Project Management for Information Technology Standard

Policy

Due to the nature and scale of the projects defined as information technology (IT) projects, it is critical that project management practices be employed and that processes are in place, increasing the probability of delivering quality solutions on time and within budget.

Purpose

This standard ensures accountability for the resources allocated to IT projects and ensures that a consistent approach is used to manage these projects.

Definitions

For the purposes of this standard:

“Project management” is the application of knowledge, skills, tools, and techniques to project activities to meet project requirements. Project teams can achieve the outcomes by using a broad range of approaches (e.g., predictive, hybrid, adaptive).

A “project” is defined as a temporary endeavor undertaken to create a unique product, service, or result. Projects can stand alone or be part of a program or portfolio.

A “program” is defined as related projects, subsidiary programs, and program activities that are managed in a coordinated manner to obtain benefits not available from managing them individually. For example, a large quantity of work may be broken down and executed as multiple projects either simultaneously or sequentially in support of common program-based business objectives. Although each project may initiate or close at different times, it isn’t until all projects are completed that the objectives or outcomes of the program are achieved. In this standard, all actions that apply to the term “project” also apply to programs.

A “portfolio” is a grouping of projects, programs, subsidiary portfolios, and operations managed as a group to achieve strategic objectives. For the purposes of this standard, portfolio does not refer to a software application portfolio, or other technical portfolio.

A “project manager” is the person assigned to lead the project team that is responsible for achieving the project objectives. Project managers perform a variety of functions, such as facilitating the project team work to achieve the outcomes and managing the processes to deliver intended outcomes.

A “project sponsor” provides leadership to the project. The sponsor links the project to the strategy for why the project is being conducted. The sponsor is intimately involved with either setting or understanding the vision, goals, and expectations of the project, and is tasked with communicating these to the project team. The sponsor also helps to secure resources, keep the project aligned to business objectives, and drives the resolution of project conflicts.

An “oversight committee” is a meeting where senior stakeholders monitor the overall status of the project and make recommendations regarding project decisions, including negotiation and execution of contracts, approval of project budgets, implementation of project schedules, assessment of project quality, and consideration of scope changes. (For major IT projects certain parameters for membership and decision-making are defined in Century Code and are further clarified in this standard.)

Certain definitions above are quoted, paraphrased or modified from:

> Project Management Institute. 2021. The Standard for Project Management (PMBOK GUIDE). 7th ed. Project Management Institute.

Guidance

Guidance related to NDCC § 54-35-15

NDCC § 54-35-15 defines what makes a project qualify as a “major project.” The italicized text that follows details how those parameters are met:

For the purposes of this subsection [NDCC § 54-35-15.2], a major project is an information technology project that meets one or more of the following criteria, as determined by the chief information officer:

a. An estimated total cost, as defined by the information technology department, of five million dollars or more;

A project's total cost is comprised of the budget required to complete all phases of the project, or collection of projects in a program environment. All phases means work required for initiating (including all procurement activities), planning, executing, and closing the project or program. If licensing, subscription fees, or other costs must be paid prior to solution go-live, those costs are included.

b. Requires one year or longer to reach operational status; or

One year of operational status is defined as the time from the signing of the contract or statement of work to the full implementation of a technology solution for any individual project. For programs, this means the signing of the contract or statement of work for the first project or phase, through the full implementation of a technology solution for any final project or phase of the program.

c. Requires oversight due to its potential benefits, risks, public impact, visibility, or another significant reason.

The North Dakota Information Technology Department (NDIT) Chief Information Officer (CIO) makes this determination.

If a project meets the criteria of any of the conditions defined in a, b, or c, above, then it is a major project.

Guidance related to NDCC § 54-59-32

NDCC § 54-59-32 establishes the need for an Oversight Committee for major IT projects. The following guidance describes how an Oversight Committee shall be assigned and how frequently it may meet, as well as how projects not defined as major IT also may be assigned an NDIT project oversight analyst or NDIT project compliance coordinator.

For projects determined to be major IT projects, an Oversight Committee must be appointed with the consideration of the named positions in NDCC § 54-59-32. The CIO shall designate one of the committee members the chairperson. Committee membership is not limited to those positions named in the statute. The director of the agency sponsoring the project, the director of OMB, and the CIO shall work together to determine the membership of each project's Committee. The Oversight Committee shall meet at least quarterly. If the project status is within ten percent of the current baseline for budget and schedule, and if there are neither change requests for review, nor high priority risks, issues, or decisions that are active, the committee may be sent a status report by the project manager in lieu of the quarterly meeting requirement.

Projects not designated as major IT, but with budgets $100,000 and up, will be assigned a project compliance coordinator from within the NDIT project management office. The NDIT project compliance coordinator's role in this scenario is to ensure that state project management best practices are followed, and that project information is kept current by the designated project manager, including a schedule that is maintained in the state's enterprise project portfolio management system, ND VIEW.

NDCC § 54-59-32.2 states that "The ... primary project manager for a major information technology project must meet the qualifications established by the department [NDIT] ..."

The "primary project manager" is defined as the lead program or project manager assigned to a major IT project who is the person responsible for ensuring the project team completes the project successfully by resolving the strategic problems/needs of the business that led to the origination of the project. This role is also the primary connection between the project team and the sponsor. The primary project manager develops the program or project plan with the team and oversees the team's performance of project activities. The primary project manager is also responsible for securing acceptance and approval of deliverables from the sponsor and stakeholders.

Following are the qualifications for the primary project manager assigned to a technology project:

For projects with budgets under $100,000 there are no specific requirements.

For projects with budgets between $100,000 and $2 million the program/project manager must demonstrate prior experience managing at least one project of similar size, scale and complexity.

For projects with budgets over $2 million, the program/project manager also must hold the Project Management Institute's Project Management Professional (PMP) certification.

For projects that qualify as a major IT project, in addition to holding the Project Management Institute's Project Management Professional (PMP) certification, the project manager must also have previously managed or co-managed an information technology project budgeted for at least $2 million, which must have spanned at least a 12-month timeline, been subject to this state standard, and had complexities requiring coordination of work between multiple entities.

Primary program/project managers assigned to major information technology projects who are not internal state staff must be contracted, assigned, and supervised through the NDIT Project Management Office. Program/project managers who are part of a vendor-based software solution team tasked with managing that company's portion of the project are exempted from this requirement.

Standard

All information technology projects shall comply with the following directives:

1. All projects shall submit an Initiative Intake request through the NDIT Self Service Portal (ServiceNow).
2. A person shall be identified to fill the project manager role.
3. A person shall be identified to fill the project sponsor role.
4. Project managers are required to utilize the North Dakota Information Technology (NDIT) Project Management Office (PMO) Project Management Checklist and related templates in the management of their projects. Contact the PMO for guidance on required templates.
5. The project manager shall maintain an electronic project document repository to manage and retain critical project documents.
    1. Documents must be stored on an electronic platform owned and managed by the State. The State's Microsoft Teams environment is preferred.
        1. Documentation to be retained in the repository includes:
        2. All documents identified in this standard, including the Project Charter, Project Plan, Post Implementation Report, and Startup and Closeout Reports.
    2. Products of project management, e.g., meeting minutes, scope change documentation.
    3. Unless NDIT is managing the project, or your agency has its own project records retention schedule, upon completion, all documentation must be retained for a period of three years, and then sent to state archives, per General Project Records Retention Schedule 801201.
        1. NDIT-managed projects will retain documentation for a period of six years after completed, per Information Technology Department Retention Schedule 801203, Project Working Papers.
6. A project charter shall be developed and executed to initiate the project, to document the business need and project objectives, and to secure commitment for the resources (e.g., human, financial, equipment) necessary for the project.
7. A project plan shall be developed as the primary planning document for the project.
8. The project budget, schedule, and scope shall be baselined once the initial project planning is completed.
    1. Revised budget or schedule baselines will be done only upon scope changes (add or remove) and the re-baseline shall include only the new or removed scope and those activities impacted by the new or removed scope.
9. During execution of the project, project status must be updated a minimum of every two weeks, unless approved by the PMO.
    1. The status report shall include the budget and schedule (including progress against budget and schedule baselines), and information on issues and risks.
    2. Throughout the life of the project, if changes occur which would impact the project objectives, or changes to cost, schedule, scope, or quality, those impacts shall be included in the project status report.

    The project shall have a closeout meeting to document project outcomes (e.g., whether or not the objectives were met), final project status information, and lessons learned.

All information technology projects with budgets of $100,000 and over shall comply with the following additional directives:

11. The project must be assigned either an NDIT Project Compliance Coordinator, or an NDIT Oversight Analyst.
    1. More information regarding the role of NDIT project oversight may be found on the Project Management Oversight web page.
12. Procurement materials must be monitored by the NDIT Project Compliance Coordinator or Oversight Analyst to allow timely and regular evaluation against the major IT project definition per NDCC § 54-35-15.
    1. If the NDIT Project Compliance Coordinator or Oversight Analyst determines that the project will become a major IT project, the Oversight Committee and the procurement collaboration team as defined in NDCC § 54-59-32 must be established.
13. The project information, schedule, budget, risks, issues, and change requests shall be entered and maintained within the State's Microsoft Project Online project and portfolio management tool, ND VIEW, adhering to the PMO Scheduling Best Practices.
14. The project information and status will be pulled into the ND VIEW dashboards.
15. The project charter and project plan (including the project schedule) must be peer-reviewed by the NDIT PMO.

    Any project replanning effort to modify the baseline without new or removed scope must be reviewed by the NDIT PMO.

All information technology projects designated as "Major Projects" shall comply with the following additional directives:

17. An Oversight Committee must be established to provide management support to the project, per NDCC § 54-59-32.
18. The project shall be assigned an NDIT Oversight Analyst.
19. The Oversight Committee must meet a minimum of quarterly or on a more frequent basis as defined by the membership of the Committee. See Guidance related to the Oversight Committee earlier in this document for certain exceptions.
20. The primary project (or program) manager must be assigned by the NDIT PMO. See Guidance related to NDCC § 54-59-32.2 earlier in this document for specific requirements.
    1. Project managers and procurement officers must meet qualifications established by the Information Technology Department and the Office of Management and Budget.
21. The Oversight Committee must meet during project initiation to determine which project artifacts they shall review, and to determine how frequently they will meet.
22. The project sponsor shall formally approve the project charter and the project plan.
    1. Prior to being approved, the Oversight Analyst assigned to the project shall review the charter for general compliance with best practices.
    2. After approval by the Oversight Analyst, and prior to any planning, vendor contract signing, or execution activities, a copy of the approved project charter shall be submitted to the Oversight Analyst assigned to the project.
23. A Project Startup Report shall be prepared.
    1. The intent of this document is to convey information from the project charter and project plan to the Legislative IT Committee at the time when the project planning has completed and the project is entering the execution phase. The information contained in this document should not be new. It should be taken from the existing referenced documents.
    2. The reported budget and schedule will be used to calculate variance during execution of the project.
    3. This report is due within two weeks of submission of the final project plan and is submitted to the OA assigned to the project.
24. Variance to baselined budget or schedule will be measured for the duration of the project as entered into ND VIEW.
25. A portfolio status report of major IT projects that includes an overview summary of each program and its related projects, as well as each individual project, will be pulled from ND VIEW for the Chief Information Officer to submit to the Legislative Information Technology Committee (LITC) on a quarterly basis.
26. If project costs exceed the baselined budget by twenty percent or more, or if the project schedule extends beyond the baselined schedule by twenty percent or more, a report must be drafted by the project manager that specifies corrective measures being undertaken to address any cost or schedule issues. This report is submitted to the Oversight Analyst, who along with a representative from the project team, shall review this information with the CIO. If the project team has not taken adequate corrective measures within ninety days after this initial report, a subsequent report shall be drafted by the project manager and submitted to the Oversight Analyst, who shall forward the report to the LITC. The project sponsor, or other agency representative, shall be summoned to testify to the committee regarding a recovery strategy for the project.
27. A Post Implementation Report (PIR) shall be completed within six months of reaching the execution complete milestone in order to assess the success of the project and to capture historical information.
    1. The Oversight Committee shall review the PIR.
    2. Prior to submission to the Oversight Committee, the Oversight Analyst assigned to the project shall review the PIR for general compliance with best practices.
    3. A copy of the final PIR shall be submitted to the OA assigned to the project.
28. A Project Closeout Report shall be created.
    1. The intent of this document is to convey information gleaned from the Post Implementation Report to the Legislative IT Committee at the time when the project has completed the closeout phase. The information contained in this document should not be new. It should be taken from the existing referenced documents.
    2. Variance to both the original planned and final approved budget and schedule will be calculated.
    3. This report is due within two weeks of submission of the PIR and is submitted to the OA assigned to the project.

Applicability

According to North Dakota Century Code, this standard applies to all executive, legislative, and judicial branch agencies. Applicable code includes: NDCC§ 54-10-28 , NDCC § 54-35-15 , NDCC §54-59-02 , NDCC §54-59-05 , NDCC §54-59-11.1 , NDCC §54-59-23 , NDCC § 54-59-32 .

The State Board of Higher Education will maintain a separate standard in accordance with NDCC § 15-10-44 .

Non-Compliance

Non-compliance of this standard shall be reported to the State Auditor's Office and the Legislative Council. Non-compliance may result in the suspension of any IT funding associated with the project.

Number: POL0020207
Revision Number: 7
Revision Date: 2025-05-30
Effective Date: 2004-12-31
Last Reviewed: 2025-05-30

Project Management Solutions Standard

Purpose

Standardize the solution(s) to provide the enterprise with Project Management software solution(s) to manage projects.

Standard

1. Microsoft Project Online will be used to fulfill projects with that need advanced project management features, resourcing management needs, and financial needs.
2. Microsoft Project for the web will be used to fulfill smaller project management needs that don't require advanced features.

Definitions

Project Management - Project management has the capacity to help plan, organize, and manage resource tools and develop resource estimates.

Microsoft Project Online - this solution is sometimes referred to as Project Web App (PWA).

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020181
Revision Number: 2
Revision Date: 2022-09-16
Effective Date: 2021-04-01
Last Reviewed: 2024-09-13

Public Workstation Access Standard

Purpose

To establish a public workstation security policy which will ensure public access workstations are protected and to minimize the risk of unauthorized access to the state government network.

Standard

1. All workstations located in an area of public access shall be configured to provide only the services needed.
2. Screen locking processes are not required.

Definition

State Government Network (Internal) - Used to outline the perimeter of the network infrastructure used solely for State Agencies and excludes other government branches, such as, K12, North Dakota universities, and other political sub-divisions attached externally to the State network.

Policy

To protect the state information technology infrastructure from unauthorized physical access.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020125
Revision Number: 1
Revision Date: 2005-07-18
Effective Date: 2005-07-18
Last Reviewed: 2024-09-13
```

Record Migration Standard

Purpose

Records will be migrated to ensure business continuity and to meet business and regulatory requirements.

Standard

State agencies must migrate electronic records to a format that can be accessed with available technology without the loss of information.

Definition

Access - Easily locate, view and use.

Record - Document, book, paper, photograph, sound recording or other material, regardless of physical form or characteristics, made or received pursuant to law or in connection with the transaction of official business.

Policy

Stored records will be migrated as necessary to ensure access when needed.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020029
Revision Number: 2
Revision Date: 2017-03-21
Effective Date: 2004-06-20
Last Reviewed: 2024-09-13
```

Remote User Access Standard

Purpose

To provide remote access capability to the enterprise network from any location, for any authorized customer without compromising the network.

Standard

1. All external connectivity to the internal state network must utilize TLS or client-based VPN.
2. All TLS or client-based VPN solutions will be provided by NDIT.
3. All TLS or client-based VPN connectivity will be authenticated and authorized by the enterprise authentication/authorization process.
4. The enterprise Multi-Factor Authentication solution will be required in conjunction with TLS or client-based VPN for remote access.
5. Remote access to the state network or state data outside the U.S. or U.S. territories shall not be allowed for team members, contractors, or third-parties.
6. Connections must be logged and monitored for unauthorized access.
7. Devices used for remote access must have up-to-date antivirus and anti-malware software.
8. Network traffic must be monitored for unauthorized access and have logging enabled.
9. Intrusion detection and prevention systems must identify threats and mitigate risk.
10. Access to Office 365 documents requires mobile device management software to govern security policies.
11. The State operates a zero-trust environment in which all users, devices, and systems must be explicitly authorized prior to permitting a connection.

Definition

Remote Access - the ability to connect to an internal network from a distant location. Generally, this implies a computer, a modem (cellular, cable, dsl, etc.), and some remote access software to connect to the internal network. Remote access means that the remote computer actually becomes a full-fledged host on the internal network.

Virtual Private Network (VPN) - a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Authentication - the process of identifying a person prior to allowing them to access some resource or service. Authentication in this context is usually a userid and password.

Authorization - the process of granting a person access a protected resources or service.

Multi-Factor Authentication (MFA) - is an approach to authentication which requires the presentation of two or more of the three authentication factors: a knowledge factor ("something only the user knows"), a possession factor ("something only the user has"), and an inherence factor ("something only the user is").

Guidance

1. Authentication and authorization for remote access to servers will be provided by enterprise managed central authentication services.
2. User IDs shall be maintained within the enterprise-managed central authentication services.
3. NDIT will provide TLS or client-based VPN to the requesting agency. The VPN will be configured to be able to access only pre-authorized hosts.
4. Use only enterprise-approved devices for remote access to VPN.
5. Mobile devices used to access Office 365 documents require MFA and mobile device management to govern security policies.

Policy

To provide users remote access to the enterprise network and attached hosts.

Scope

This standard applies to all executive branch state agencies including the University Systems Office and entities performing actions on their behalf, e.g. vendors.

Higher education institutions beyond the University Systems Office are excluded, e.g. campuses and agricultural and research centers.

This standard is designed to ensure the integrity of the wide area network, therefore it applies to all entities currently using wide area network services.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Exceptions

In cases where agencies have team members that have a need to conduct business internationally (outside U.S. or U.S. territories), a request must be submitted three weeks prior to travel. The request shall be submitted by the team member's HR to NDIT using ServiceNow and submitted as a generic service request.

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Noncompliance to this standard has been classified as high-risk i.e. having impact on the integrity of enterprise information systems. Violations to this standard will result in ITD operations taking immediate action to prevent enterprise risk prior to the reporting of non-compliance to the Office of the State Auditor.

```
Number: POL0020126
Revision Number: 9
Revision Date: 2025-01-06
Effective Date: 2004-05-12
Last Reviewed: 2025-01-06
```

Supply Chain Risk Management Standard

Purpose

To protect state data, systems, and supply chain information and communications technology (ICT) through third-party risk management (TPRM).

Standard

North Dakota state government branches, agencies, and entities are required to ensure that any IT procurements that involve a vendor handling, storing, and/or transmitting state data undergo a NDIT third-party assessment.

1. **Third-Party Risk Assessment:**

Third-party risk assessments, also known as supply chain risk assessments, provide organizations with visibility into supply chain risks and allows organizations to respond appropriately to any identified risk.

Any organization IT procurement is required to be integrated into the State's Third-Party Risk Management (TPRM) and undergo a risk assessment. Continuous risk assessments will occur, as needed.

Definitions

Information and Communications Technology – Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.

Supply Chain – Organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations, and maintenance, and/or disposal of systems and system components. Also, referred to as third-party vendor management.

Supply Chain Risk Management – A systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures.

Supply Chain Risk Assessment – A systematic examination of cybersecurity risks throughout the supply chain, likelihoods of their occurrence, and potential impacts.

Policy

To provide security and privacy best practices for third-party vendor management.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e., campuses and agricultural and research centers.

State of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09). Policy and standards for procurement by state agencies should also be established following ND Century Code (Chapter 54-59-05) .

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Resources

- National Institute of Standards and Technology (NIST)

- NIST Special Publication (SP) 800-161 Revision 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- NIST Cybersecurity Supply Chain Risk Management (C-SCRM)

Revision Table

Date	Authored by	Approved by	Version	Description of Change
06/13/2023	Kathleen Peery	NDIT Management	1.0	Initial Creation of Standard

---

```
Revision Number: 1
Revision Date: 2023-06-13
Effective Date: 2023-06-13
Last Reviewed: 2023-06-13
```

Talent Management Standard

Purpose

Standardize the solution to provide the enterprise with the ability to manage accounts payable.

Standard

1. PeopleSoft Human Capital Management Suite from Oracle; will be used to fulfill talent management business needs.

Definitions

Talent Management - Talent management is the full scope of HR processes to attract, onboard, develop, motivate, and retain high-performing employees.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020178
Revision Number: 1
Revision Date: 2021-04-06
Effective Date: 2021-04-06
Last Reviewed: 2024-09-13

Training Course Development Standard

Purpose

Standardize the solution to provide the enterprise with the ability to create online training courses that will be loaded to an learning management system (LMS).

Standard

1. Articulate 360 from Articulate; will be used to fulfill the training course development business needs.

Definitions

Training Course - A training course is a series of lessons or lectures teaching the skills you need for a particular job or activity.

Learning Management System (ELM) - Enterprise Learning Management is a platform used to manage and track employee learning and training information. It allows self-service access for all types of users including learners, managers, instructors, training coordinators and administrators. The system can track the learning catalog, as well as user's training history and transcript.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020240
Revision Number: 1
Revision Date: 2021-03-08
Effective Date: 2021-03-08
Last Reviewed: 2024-09-13

Virtual Event Management Standard

Purpose

Standardize the solution to provide the enterprise with a Virtual Event Management solution.

Standard

1. vFairs Virtual Conference Platform provided by vFairs LLC will be used to fulfill virtual conference business needs.

Definitions

Virtual Event Management - A virtual event, also known as an online event, virtual conference or live stream experience, is an event that involves people interacting in an online environment on the web, rather than meeting in a physical location.

Popular uses of virtual events include webinars, live streams, virtual trade shows, online classes, online tours and company events. Hybrid events have also become popular in recent years, mixing in-person events with virtual content accessed online.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Number: POL0020247
Revision Number: 1
Revision Date: 2022-08-10
Effective Date: 2022-08-10
Last Reviewed: 2024-09-13

Virtual Meetings Standard

Purpose

Standardize the solution to provide the enterprise with the ability to conduct meetings digitally.

Standard

1. Teams from Microsoft; will be used to fulfill the need to conduct virtual meetings.

Definitions

Virtual Meetings - A virtual meeting is a meeting that takes place online rather than physically with the participants in the same room.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020188
Revision Number: 1
Revision Date: 2021-05-12
Effective Date: 2021-05-12
Last Reviewed: 2024-09-13
```

Voice Services for Non-Standard Users

Purpose

Standardize the solutions to provide the enterprise with the ability to manage Voice Services for Non-Standard users.

Standard

Mobile Centric users - Core requirements for this subset of users are cellular based and require PBX like features.

1. OneTalk from Verizon; will be used to fulfill the business Voice needs of these Non-Standard users.
2. Telephone numbers will not be ported to Verizon. (Example - Use Lumen Mobility Feature and forward calls to Verizon Hunt Group or AA lead number.)
3. OneTalk physical phones may be deployed in either LTE or LAN mode.
4. OneTalk feature set can be applied to Mobile phones with desk phones as an optional addition.
5. Verizon Hunt Group or Auto Attendant numbers are not to be published as a lead number for the line of business. A state provided Lumen number should be used and billed accordingly.

Office Centric users - Traditional set of standard PBX feature requirements including analog but the user base falls into the Non-Standard user category.

1. BEK Connect, will be used to fulfill the business Voice needs for these Non-Standard users.
2. Telephone numbers can be ported to BEK. (BEK has agreed to protect our unused numbers so that they are not lost.)
3. Full BEK Connect suite of services, desk phones and analog lines are available in this offering.
4. BEK Connect services can be installed on STAGEnet provided network or any available network.
5. Configuration and support are provided by BEK but coordinated by NDIT.

Definitions

Standard User - Any user that is either assigned to or employed by an agency covered under ND Century Code such as Executive, Legislative, and Judicial branch agencies.

Non-Standard User - Any user that is neither assigned to, nor employed by an agency covered under ND Century Code such as Executive, Legislative, and Judicial branch agencies. But who's agency, board or commission has opted to utilize ND Voice Services. This also could be a user that has a defined feature use case that the standard offering does not meet.

Mobile Centric Users - These users are highly mobile. May not even have an office they use regularly. Mobile phone is the primary method for communication.

Office Centric Users - These are traditional office workers at a permanent location. They may still have the need for a desk phone, Desktop client or mobile app for telephone communication.

Scope

This standard applies to all Agencies, Boards and Commissions that have opted to utilize ND Voice Services.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

Revision Number: 1
Revision Date: 2025-01-23
Effective Date: 2025-01-23
Last Reviewed: 2025-01-23

Voice for Standard Users

Purpose

Standardize the solutions to provide the enterprise with the ability to manage Voice Services for standard users.

Standard

Microsoft Teams Voice - Will be used to provide for core requirements of PBX like features.

Enterprise Voice user - Requires G5 or Office Premium license from MS. An active nd.gov account for the user. A state provided Direct Inward Dial number will be provided for each user.

Common Area Phones - Physical phone for shared locations that aren't owned by a named user.

Auto Attendants - Standard voice auto attendants will be created in MS Teams.

Basic Call Queues - Standard call queue and hunt group features will be created in MS Teams.

Analog lines - Analog lines for uses other than Fax, Elevator or Security system shall be provided with Teams analog media gateway.

Teams physical phone device - Yealink MP56 is the standard for Teams.

Definitions

Standard User - Any user that is either assigned to or employed by an agency covered under ND Century Code such as Executive, Legislative, and Judicial branch agencies.

Non-Standard User - Any user that is neither assigned to, nor employed by an agency covered under ND Century Code such as Executive, Legislative, and Judicial branch agencies. But who's agency, board or commission has opted to utilize ND Voice Services. This also could be a user that has a defined feature use case that the standard offering does not meet.

Scope

This standard applies to all Executive, Legislative, and Judicial branch agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Revision Number: 1
Revision Date: 2025-01-25
Effective Date: 2025-01-25
Last Reviewed: 2025-01-25
```

Vulnerability Management Standard

Purpose

The purpose of this Vulnerability Management Standard is to establish a structured approach for identifying, assessing, prioritizing, and remediating security vulnerabilities across NDIT's infrastructure. It ensures that security risks are systematically managed to reduce the likelihood of exploitation and maintain compliance with industry regulations and best practices.

Standard

REDACTED - Contact NDIT for more information

Revision Number: 1.1
Revision Date: 2025-05-20
Effective Date: 2025-05-20
Last Reviewed: 2025-03-12

Web Content Management System Standard

Purpose

Standardize the solution to provide the enterprise with the ability to manage web content management system.

Standard

1. State website platform built on Drupal and customized by Information Technology Department; will be used to fulfill web content management business needs.

Definitions

Web Content Management - A web content management system is a software content management system specifically for web content. It provides website authoring, collaboration, and administration tools that help users with little knowledge of web programming languages or markup languages create and manage website content.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020171
Revision Number: 1
Revision Date: 2021-04-06
Effective Date: 2021-04-06
Last Reviewed: 2024-09-13
```

Web Development Standard

Purpose

Create a common, compliant framework for development of accessible web sites that support the function and mission of the entity while establishing a level of effectiveness, consistency and professionalism across the State of North Dakota web sites.

Standard

1. HTML shall validate to a World Wide Web Consortium's "W3C Recommendation".
2. Cascading Style Sheets (CSS) shall validate to a "W3C Recommendation".
3. Every public web site HTML page shall display the state banner.
   Advertisements shall not be displayed.

   Links to business partners are allowed if they meet all of the following:

   1. Link is related to the agency/department's business
   2. It is without compensation
   3. There is no discrimination in determining allowed links

   Business partner sites are not subject to state standards, however they must comply with the following:

   1. Cannot display state banner
   2. Shall not appear as an official state government agency

   Every public web site HTML page shall provide a link to or display the following:

   1. Contact information including address, phone and email
   2. Privacy policy
   3. Home page
   4. Security policy
   5. Disclaimer

Definition

Advertisement - Blatant advertisement - i.e. selling of advertisement on web site Graphics (such as logos) - links or information that endorse a business or organization. The inclusion of vendor logos and links to commercial sites with the intent to promote sales.

Business Partner Sites - A third party site providing information/applications/services on behalf of the state related to the services of the agency for the benefit of the public that is not hosted on state servers and is not directly controlled by a state agency.

HTML pages - Any page that contains HTML code. This includes static or generated pages.

Intranet web site - Web site that is only accessible to an agency's staff.

Web site - A web site is a collection of web files or application generated web pages.

Public web site - A site accessible by the general public.

Applicable North Dakota Century Code (NDCC)

The Great Seal of North Dakota is reserved for official use. Refer to NDCC 54-02-01 for regulations. For accessibility information - Refer to NDCC 14-02.4-14 and NDCC 14-02.4-15 for definitions of discrimination in the provision of public services.

Guidance

1. W3C specification for HTMLhttp://www.w3.org/TR/#tr_HTML
2. W3C specification for Cascading Style Sheetshttp://www.w3.org/TR/#tr_CSS

Policy

Implementation of development standards for accessible, consistent, and user-friendly web sites providing quick, simple access to government information and services. Thereby, reducing costs and streamlining government by providing greater access to information and more convenient government services.

Scope

This standard applies to all executive branch state agencies including the University Systems Office but excluding other higher education institutions, i.e. campuses and agricultural and research centers.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Non-Compliance

Non-compliance with this standard shall be reported to the Office of the State Auditor.

```
Number: POL0020014
Revision Number: 9
Revision Date: 2022-08-10
Effective Date: 2004-11-02
Last Reviewed: 2024-09-13
```

Zero Trust Standard

Purpose

This standard exists to provide guidance on the enterprise standards for zero trust security.

Principles:

- All traffic, users, and applications are always assumed to be compromised. There is no such thing as a 'trusted service.'
- There should always be 2 independent layers of security, controlled by 2 independent teams (with separation of duties)
  - Layers of security include identity, firewalls, ACL's, conditional access, application controls, etc...
- The 'blast radius' (potential lateral movement ability) should be minimized to the smallest possible margin.
- Admins, users, services, and networks should always be configured according to the 'principle of least privileges'
- Layer 7 rules should be used where possible.
- Blacklisted firewall rules should be avoided at all costs and only used for generic threat blocking. All firewalls should be based on whitelisting concepts.

Standard

User space

1. If the user's gateway is not a IDS/IPS/L7 firewall, all user traffic must pass through at least 1 IDS/IPS/L7 firewall after traversing the initial gateway.
2. NAT/PAT must be utilized wherever possible for all government/K12/PSD traffic

Server space

NDIT utilizes a zero-trust microsegmentation architecture for all servers

1. All server traffic to/from the internet or user-space must pass through at least 1 IDS/IPS/L7 firewall
2. All unrelated server-to-server traffic must be segmented where possible

Cloud based PaaS/SaaS services must be protected 2 independent layers if not protected by a IDS/IPS/L7 firewall.

1. To protect from a compromised identity, the 2 layers must be managed by non-overlapping accounts
2. Non-network controls (identity/certificates) may only be used for one layer. A network based control must also be present.

Scope

The standard applies to all STAGEnet traffic.

Statement of Commitment

North Dakota's CIO/CTO directs that IT Policy be created to establish statewide information technology policies and standards as defined within ND Century Code (Chapter 54-59-09).

Number: POL0030003
Revision Number: 1
Revision Date: 2024-09-16

Effective Date: 2024-09-16
Last Reviewed: 2024-09-16