

NEVADA DEPARTMENT OF TRANSPORTATION

CLOUD TECHNOLOGY POLICY



POLICY No.

TP 1-3-13

PURPOSE

The purpose of this policy is to define governance of cloud technology usage in support of the Nevada Department of Transportation (NDOT) “Cloud Smart” approach. This policy is designed to protect NDOT and its Users from inappropriate cloud use that may expose NDOT to risks which compromise the confidentiality, integrity, and availability of our network and data.

POLICY

As of January 2021, NDOT has adopted a “Cloud Smart” approach for all new services, systems, and solutions. This means NDOT will consider cloud computing technology first where appropriate when deploying or refreshing technology.

This policy:

1. Establishes Microsoft Azure as NDOT’s chosen cloud vendor. Other cloud services may be considered through written request, which will be reviewed and approved by NDOT.
2. Establishes Platform as a Service (PaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Integration Platform as a Service (iPaaS), and Function as a Service (FaaS) as NDOT’s chosen cloud service types. As technology advances, additional new cloud solution types may be considered and would be subject to NDOT review and approval.
3. Establishes that any cloud computing used must meet security, access controls, networking, interoperability, integration, data governance, audit, and continuous system management requirements in accordance with the NDOT Information Technology (IT) Standards.
4. Establishes Cloud Data Ownership: NDOT decrees that all NDOT Data being collected, stored, passed through, or reported out of a vendor-supported or third-party cloud-hosted application, system, or service is considered the NDOT’s intellectual property, meaning it is an NDOT asset and NDOT owned. NDOT ownership includes the right to have the NDOT Data made available to retrieve, audit, report from, or share, at all times according to the conditions set in the contract and or the Data Sharing Agreement (DSA).
5. Establishes any use of NDOT Data in a cloud environment maintain the ability to protect the confidentiality, integrity, and availability of the NDOT Data, and comply with other general cloud requirements, as defined in the NDOT IT Standards and the TP 3-11 Data Governance Policy. Additional guidance is found in the Nevada Revised Statute (NRS) 603A Security and Privacy of Personal Information, S.5.06.01 State of Nevada Standard Cloud Services, and the Center for Internet Security (CIS) v8.
6. Establishes Timely Access:
 - **System Access:** Systems remain available to NDOT, with the appropriate permissions, in support of NDOT business needs, as agreed upon in the Service Level Agreement (SLA) set in the contract.
 - **Data Access:** All NDOT Data stored in the cloud must be available to NDOT at all times. NDOT maintains all rights to access, audit, perform security checks, and retrieve NDOT Data from vendor-

supported or third-party cloud-hosted applications, systems, or services. The vendor or third-party has been chosen as a trusted entity to store and safeguard NDOT Data, but it is not the data owner, and may not, therefore, prevent authorized personnel from accessing, auditing, performing security checks, or retrieving NDOT Data, according to NDOT's needs.

7. Establishes Access Issue Resolution Process: In the event an issue occurs restricting or impeding an NDOT user from timely access to the cloud system and its data, the provider must provide a resolution according to the SLA set in the contract, to minimize the impact to NDOT business and IT operations.

1. DEFINITIONS

- 1.1 Business Information – Any data created and/or managed by 1) NDOT Systems, and/or 2) NDOT employees, contractors, and/or consultants within the scope of the employees' work responsibilities.
- 1.2 Cloud Computing – Cloud computing can be defined as the utilization of cloud resources hosted by third parties or NDOT in locations which may or may not be fully owned or controlled by NDOT.
- 1.3 Cloud Computing Model – A computing model that allows for easy, on-demand computing resources (networks, servers, storage, applications, and services) that can be quickly provisioned and de-provisioned with minimal interaction and are accessible to the users via the internet. Cloud Computing Model types include private clouds (dedicated resources for one user or group), public clouds (resources shared across users but not owned by the end user), hybrid clouds (combined environments of private and public clouds), multiclouds (use of multiple cloud services from different vendors), StateRAMP certified clouds (state-approved clouds with specified security controls), and FedRAMP certified clouds (government-approved clouds with specified security controls).
- 1.4 Cloud Services – The service model that defines how each Cloud Computing Model operates. Each type offers a different level of vendor control and security protection over an organization's data. Cloud Service types include PaaS (platform to run custom applications), SaaS (fully managed software services), IaaS (infrastructure resources like virtual machines and networks), iPaaS (tools for integrating data across environments), and FaaS (modular code development and microservice deployment).
- 1.5 Commodity – an out of the box tool or technology that has not been designed specifically for NDOT and has not been modified for NDOT's use.
- 1.6 NDOT Data – Information contained in either NDOT computer systems, cloud storage, or as a physical copy that is utilized for NDOT purposes. NDOT Data includes both structured data (including spatial and non-spatial data) and unstructured data (such as reports, materials, studies, photographs, negatives, drawings, videos). Structured data conforms to a defined format or data model making it easy to perform searches, analytics, and reporting. Whereas unstructured data does not conform to conventional data model formats and is more frequently stored as finished end products.
- 1.7 Department Systems – Computing devices and their related software created, owned, and/or licensed to NDOT that are used to store or process NDOT Data.
- 1.8 Professional Service – a tool or technology specifically designed for NDOT, and modifications are made to suite NDOT's specific needs.

1.9 User – All NDOT employees, volunteers, interns, third-party vendors, and contractors that have access to NDOT Data.

2. BACKGROUND

Cloud resources are valuable tools that allow NDOT Users to store large amounts of information and perform collaborative tasks more effectively. However, there are risks that must be mitigated to properly ensure the confidentiality, integrity, and availability of NDOT Data for any and all tasks. Some of the risks that must be addressed are data classification and retention, data ownership, disaster recover, security incident handling responsibilities, audits, and reporting and data sharing. This policy provides the framework within which NDOT Users will be expected to operate when utilizing cloud computing technologies.

3. SCOPE

- 3.1 This policy applies to all Users authorized to access, manage, or store NDOT Data, in any manner while executing business functions, activities, or services for or on behalf of the NDOT, its covered entities, its third-party vendors and contractors, shall be required to comply with this policy.
- 3.2 This policy applies during all times and at all locations used for NDOT business whether working in an NDOT office or working remotely as supported by the TP 1-3-14 Technology Use Policy.
- 3.3 This policy applies to the evaluation and assessment of risk, safety, value of using PaaS, SaaS, IaaS, iPaaS, and FaaS cloud service types.
- 3.4 This policy applies to the procurement of vendor-supported or third-party cloud-hosted services, which may be implemented and provisioned by following the S.5.06.01 State of Nevada Standard Cloud Services, S.6.05.01 State of Nevada Standard Secure Software Configuration, and NDOT's IT procurement process. NDOT is responsible for ensuring all appropriate controls for purchasing and contracting cloud computing technologies are in place and are properly authorized. To procure these services requires contractual provisions on the use and protection of data. A S.5.06.01.F Cloud Services Assessment Worksheet will be completed by the vendor or third-party to ensure the proper safety and security controls are in place for the acquired cloud solution and services.
- 3.5 This policy applies to the protection and security of NDOT Data being stored, transferred, or shared within and between cloud environments. NDOT shall adhere to the NDOT Data Classification Policy when classifying systems and NDOT Data being stored, transferred, or shared within and between cloud environments. Refer to the NDOT IT Standards document for additional guidance. Secure access to confidential, restricted, and/or sensitive NDOT Data within and between cloud environments must be a controlled process in alignment with the Nevada Revised Statute (NRS) 603A Security and Privacy of Personal Information, in compliance with Center for Internet Security (CIS) v8.
- 3.6 This policy supports the management of network resources utilizing cloud technologies, in compliance with the NDOT IT Standards and S.5.06.01 State of Nevada Standard Cloud Services.
- 3.7 Exceptions: Requests for exceptions to State of Nevada Standards shall be submitted to the State Chief Information Security Officer (CISO). Requests for exceptions to this policy shall be submitted in writing to the NDOT Chief Data Officer (CDO), NDOT Chief Information Security Officer (ISO), and NDOT Data Governance Manager (DGM) and shall state reasons for the exception, impact, risk, and alternate controls that will be

implemented to minimize impact and risk. NDOT exceptions shall be granted only upon approval by the NDOT CDO, ISO, and DGM.

4. RESPONSIBILITY

- 4.1 In support and enforcement of the mission and purposes of this policy, the IT Steering Committee, the Data Governance Committee, the Data Management Office, and the Information Security Office shall provide the leadership, oversight, and activities herein, with the functions of data access and usage shared among NDOT executive and senior sponsors, data stewards, data administrators, data users, and data owners.
- 4.2 The vendor and NDOT have a shared responsibility to manage and enforce the confidentiality, integrity, and availability of NDOT Data and systems. Cloud security is mandated by the Federal Information Security Modernization Act (FISMA). The National Institute of Standards and Technology (NIST) provides the standards. The Cybersecurity and Infrastructure Security Agency (CISA) provides technical guidance to support implementation. The Federal Risk and Authorization Management Program (FedRAMP) authorizes services to be used by any federal and state agencies. Other policies and guides to reference include the operations policies, operations Standard Operating Procedures (SOPs) and Guides, and the S.5.06.01 State of Nevada Standard Cloud Services.
- 4.3 The vendor will provide ongoing service support as set in the SLAs of the contract.
- 4.4 All Users who utilize cloud computing technologies for storage and/or processing of NDOT Business Information and/or any NDOT Data must utilize only NDOT approved and contracted cloud services for such activities.
- 4.5 Users must obtain Information Technology (IT) Division approval of cloud computing technologies prior to contract approval.
- 4.6 Personal-use cloud tools may be used to support NDOT business needs if compliant with TP 1-3-14 Technology Use Policy, the S.3.04.04.1F State of Nevada Acceptable Use Agreement, and the S.5.04.04 State of Nevada Standard Data Security Architecture.
- 4.7 NDOT Data shall be used only for business purposes and not for personal or any other purposes without prior NDOT approval.

5. PROCEDURE

- 5.1 Upon approval, this policy will be reviewed annually by the responsible parties listed in *Section 4.1 Responsibility* above, unless the need of the business requires a more frequent review.
- 5.2 The following procedures are adopted and available to Users in support of this policy:
 - 5.2.1 Cloud Procurement Procedure – this procedure describes the steps taken to procure a new cloud technology or service. Additionally, cloud service users are required to comply with S.5.06.01 - Cloud Services, as well as any additional requirements for the storage or processing of Sensitive Data prescribed in TP 1-3-14 Technology Use Policy, and TP 1-3-15 Mobile Device Policy.
 - a) NDOT or designee drafts an architecture diagram that depicts how the proposed cloud solution will fit into NDOT’s current technology landscape.

- b) NDOT requests Information Technical Committee (ITC) review and provisional approval of the architecture diagram. Review includes assessment of risk to the current infrastructure if the new cloud solution is implemented.
- c) NDOT decides if a service or commodity is needed.
- d) If a service is required, NDOT refers to the Agreement Services process on Agreement Services SharePoint.
- e) If a commodity is required, NDOT refers to the Purchasing Process, established by the Purchasing Division.

5.2.2 Interface Connection Request Procedure – this procedure describes the steps taken to establish a new interface connection between cloud service solutions.

- a) NDOT or designee drafts a data flow diagram that would show how data would be shared between the two systems, and what kind of connection is being recommended.
- b) NDOT or designee outlines the format expectations for the data to be shared.
- c) NDOT or designee drafts an architecture diagram depicting how the new connection would fit into NDOT’s current technology landscape.
- d) NDOT requests ITC review and provisional approval of the interface plans revealed in the data flow diagram, data format expectations, and architecture diagram. Review includes assessment of risk to the current infrastructure if the new connection is implemented.
- e) NDOT or designee builds the interface connection.
- f) NDOT or designee updates the as-built interface connection documentation to finalize data flow diagram, data format expectations, and architecture diagram.
- g) NDOT requests ITC review the updated documentation and provide final approval.
- h) NDOT or designee implements interface connection into production.

5.2.3 Termination and Final Data Asset Copy Request Procedure – this procedure describes the steps taken at the time of termination to request a copy of the data asset copy, the delivery method for receipt of the copy, and the certificate of destruction.

- a) NDOT elicits from the business which assets are required to be included in the final data asset copy.
- b) NDOT shares list of data assets with the vendor, and has the vendor confirm they are able to produce the final data asset copy.
- c) NDOT confers with the vendor to confirm/agree upon the format of the final data asset copy, ensuring it conforms to the data format standards in the Data Governance Requirements and Standards section of the NDOT IT Standards.
- d) NDOT and Vendor plan jointly for the delivery date, time, and delivery method, ensuring the specifics are documented and agreed upon by both NDOT and vendor.
- e) Vendor delivers final data asset copy and NDOT to confirm receipt.
- f) Vendor produces certificate of destruction for NDOT.
- g) NDOT confirms certificate of destruction and signs off on closure of service/system/agreement.

5.2.4 Audit procedure – this procedure describes the steps taken for NDOT to perform an audit of the cloud service vendor architecture referenced in the contract. Audits will be performed on an annual basis.

- a) NDOT will notify the cloud service vendor of the audit by providing the vendor with the NDOT Vendor Compliance Questionnaire for Cloud Technology form.
- b) Vendor will fill out and return the completed form to NDOT within 30 days of receiving the NDOT Vendor Compliance Questionnaire for Cloud Technology form.
- c) NDOT evaluates responses and assesses the vendor’s adherence to contractual obligations.
- d) NDOT documents non-compliance or risks, and shares feedback with vendor.
- e) If a corrective action plan is required, NDOT and vendor document a plan together.
- f) Vendor will implement corrective action plan, and provide status updates to NDOT, per the plan.

5.3 Enforcement: Any deviation from or exception to the procedures in this policy and any decision made contrary to the ITC’s decision on approved cloud technology must be signed off by the NDOT Director.

6. REFERENCES

6.1 For questions related to this policy, contact the Information Security Office and Data Management Office:

6.1.1 Information Security Office – ITSecurityGroupDL@dot.nv.gov

6.1.2 Data Management Office – dmo@dot.nv.gov

6.2 Related supporting policies and reference documents include:

Policy, Standard, or Statue	Owner	Version
NDOT IT Strategic Plan FY23-25 FY23-FY25 Strategic Plan v1.docx	NDOT CIO	v1
05GUI120A NDOT Cloud Strategy NDOT Enterprise Cloud Strategy - Cloud Center of Excellence (CCoE)	NDOT CIO	
NDOT Information Technology Standards IT Standards v3.0	NDOT CIO	v3
TP 3-11 Data Governance Policy NDOT Data Governance Policy	NDOT CDO	v1
Nevada Revised Statute (NRS) 603A Security and Privacy of Personal Information Nevada Revised Statute (NRS) 603A Security and Privacy of Personal Information	State of Nevada	
Center for Internet Security (CIS) v8 Center for Internet Security (CIS) v8	Center for Internet Security	v8
TP 1-3-14 Technology Use Policy NDOT Technology Use Policy	NDOT CIO	
State of Nevada Security Policies, Standards, and Procedures State of Nevada Security Policies, Standards and Procedures Website	State CISO & CIO	
S.5.06.01 State of Nevada Standard Cloud Services S.5.06.01 - Cloud Services	State CISO & CIO	G
S.3.04.04.1F State of Nevada Acceptable Use Agreement S.3.04.04.1F - Acceptable Use Agreement	State CISO & CIO	

S.5.04.04 State of Nevada Standard Data Security Architecture S.5.04.04 - Data Security Architecture	State CISO & CIO	
S.6.05.01 State of Nevada Standard Secure Software Configuration S.6.05.01 - Secure Software Configuration	State CISO & CIO	A
S.5.06.01.F Cloud Services Assessment Worksheet S.5.06.01.1F - Cloud Services Assessment Worksheet	State CISO & CIO	
NDOT Data Classification Policy ---placeholder---	NDOT CDO	Drafted; not approved state
Cloud Security Alliance Shared Responsibility Model Cloud Security Alliance Website	Cloud Security Alliance	
Federal Information Security Modernization Act (FISMA) 2.2521 - Federal Information Security Modernization Act of 2014 Cybersecurity and Infrastructure - Federal Information Security Modernization Act Website	Cybersecurity & Infrastructure Security Agency (CISA)	n/a
National Institute of Standards and Technology (NIST) NIST Cybersecurity Framework NIST	NIST	n/a
Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity and Infrastructure Security Agency (CISA)	CISA	n/a
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP.Gov Website	General Services Administration	
TP 1-3-15 Mobile Device Policy NDOT Mobile Device Policy	NDOT CIO	
NDOT Data Sharing Agreement Template NDOT Data Sharing Agreement Template Final v1.0	DMO	n/a

ROUTING HISTORY (This portion will be used to track the review, edit, and comment routing progress of the TP and will be deleted when finalized.)

Date	Change	Name Division
12/8/2017	V1.0 – Initial approved version	
10/15/2024	V2.0 – revised version, updated with new cloud technology criteria and data specific criteria	Edythe Logston & Yesh Purkar/DMO
11/1/2024	V2.1 – revised version, updated with feedback from ITC Committee	Edythe Logston & Yesh Purkar/DMO
11/6/2024	V3.0 – polished version; post ITC approval	Edythe Logston & Yesh Purkar/DMO

APPROVED BY	SIGNATURE	APPROVAL DATE
ITC		11/6/2024