ATTACHMENT E
General DEPARTMENT IT Standards

INTRODUCTION

The purpose of this document is to provide Nevada Department of Transportation (DEPARTMENT) vendors with the following Information Technology Standards to facilitate the implementation and management of DEPARTMENT enterprise information systems. This document will provide standards that include, but are not limited to planning, designing, building, creating, developing, enhancing, implementing, maintaining, and using DEPARTMENT networks, gateways, front ends, information systems, applications databases, computer-based tools, data, analytics, artificial intelligence (AI), and any supporting technologies, and information assets.

The following products and standards pertain to all vendors that the DEPARTMENT engages with to conduct business. The vendor's product and/or service must comply with these standards. In addition, these standards apply to any entity connecting to DEPARTMENT IT resources to conduct business. Vendors are responsible for developing and maintaining procedures to facilitate and monitor the implementation of these standards. Additionally, the DEPARTMENT's IT Division has adopted the use of Scrum as its primary project management approach across all functional areas (Application Development, Systems, Networking, etc.) and prefers vendors with familiarity and/or fluency in Agile methods, however, the DEPARTMENT's IT Division can accommodate other methodologies upon approval. The following information will provide a baseline of requirements and specifications and should be included in the completed specific projects, tasks, deliverables, or functions.

Below are the products and standards used within the DEPARTMENT – effective as of June 28, 2024. The standards are constantly changing due to technological advances at the DEPARTMENT; therefore, vendors should follow these guidelines but should also check with the DEPARTMENT's IT Division for any recent changes to the current specifications or requirements. Based upon individual project specifications, there may be additional policies, procedures, or standards to which vendors must adhere. However, these will be discussed on an as-needed basis.

CLOUD STANDARDS:

The DEPARTMENT has chosen Microsoft Azure for its primary cloud vendor. Vendor-managed cloud solutions may reside in other cloud platforms if they comply with all State of Nevada and Nevada Department of Transportation's Cloud and Security standards. All vendor-managed (IaaS, PaaS, SaaS) solutions in platforms outside of Azure must be ported to Azure by the vendor prior to transferring administration and/or ownership to the DEPARTMENT.

GENERAL CLOUD REQUIREMENTS:

To ensure the confidentiality, integrity, and availability of DEPARTMENT data, the following requirements are considered the minimum baseline for all Cloud services:

- Cloud data centers, staff, and contractors collecting, processing, transmitting, storing, or interconnecting State data in a cloud environment must be located within the continental United States.
- Multi-factor Authentication (MFA) is required for employees and contractors connecting from outside the DEPARTMENT or State private networks to a cloud service that collects, processes, transmits, stores, or interconnects with State data.
- Cloud services must enforce least-privilege and just-in-time access to data, based on access roles established or agreed to by the DEPARTMENT.
- All data must be encrypted both at rest and in transit. In these cases, the DEPARTMENT should control and manage the encryption keys where possible.
- All data must traverse the NDOT and Azure private networks unless explicitly required to be publicly available. This includes Databases, Storage Accounts, Key Vaults, etc.

- Cloud-based solutions will be deployed via code using either templates and/or scripts, manual GUI installations are to be avoided. The DEPARTMENT supports the Infrastructure as Code (IaC) methodology.
- All templates, code, snippets etc. must be presented to and approved by the Cloud Solutions Architect (CSA) before deployment.
- All cloud-based deployments must adhere to the DEPARTMENT'S tag, location, naming, and other governance standards. Systems exposed to the Internet must be secured behind a Web Application Firewall (WAF) or other security device approved by the Information Security Officer (ISO) and CSA.
- All systems must be approved by the Infrastructure Technical Committee (ITC) or Change Management Board (CAB) prior to implementation. Presentations must include full architecture diagrams, resource lists, cost estimates, etc.
- Cloud Platforms offering Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), shall demonstrate or show proof of comparable controls and processes needed to meet FedRAMP certified requirements or Center for Internet Security (CIS) controls identified as applicable to the relevant cloud service model in the current CIS Controls Cloud Companion Guide, as well as comply with applicable State and Federal security requirements for the information being collected, processed, transmitted, stored, destroyed, or interconnected.
- Cloud Data Ownership - All data created or collected by a vendor or service provider is the exclusive property of the DEPARTMENT. These standards ensure compliance with the DEPARTMENT's Records Management and Data Governance Policies. Regular audits will be conducted to verify compliance.
- Prior to authorizing use of a Cloud service, the DEPARTMENT shall conduct a formal risk assessment of the proposed connections utilizing agency risk management processes and completing the Cloud Services Assessment Worksheet available on the State information security standards webpage.

Related Documents:

NRS 603A, Security and Privacy of Personal Information State Information Security Program Policy, 100 Data Sensitivity, S.3.02.02 Information Security Risk Analysis, S.3.07.01

State Security Policies
State Cloud Services Standard

GENERAL STANDARDS:

All operating systems (OS's), applications, software components and other components must stay within two major version revisions and have support for security updates, bug fixes and patches. Obsolete and unsupported operating systems, applications, and software components are not authorized.

Data Governance Requirements and Standards

- Data Governance is a business-driven program, owned and enforced by the Nevada Department of Transportation (NDOT), Chief Data Officer (CDO), Enterprise Data and Analytics Program (EDAP), and Data Governance Team governing entities.
- Employees, volunteers, interns, third-party vendors, and contractors who access, utilize, or manage data in any manner while executing business functions, activities, or services for or on behalf of the DEPARTMENT, its covered entities, its third-party vendors, and contractors, shall be required to comply with the NDOT Data Governance Policy.
- Use encryption protocols (e.g., AES-256) for data at rest and in transit and implement multi-factor authentication (MFA) for all systems accessing sensitive data.
- Use standardized data formats (e.g., JSON, XML, and YAML) for data exchange between systems, and ensure all data integration processes use methods such as ETL (Extract, Transform, Load), ELT (Extract, Load, Transform), and CDC (Change Data Capture) tools that support data validation and transformation. Ensure that all data always remains the property of NDOT, and can be accessed without additional cost.

- Require all devices accessing internal NDOT systems from an outside network must use industry best practice secure connection, with a minimum AES-256 encryption.
- Enforce remote wipe capabilities for lost or stolen mobile devices to protect sensitive data.
- Non-NDOT devices connecting to the NDOT environment via VPN browser access, are strictly prohibited from uploading or downloading documents and data to and from the NDOT environment.
- Implement role-based access control (RBAC) to ensure users have the minimum necessary access to perform their duties.
- Ensure all data entries are validated against defined rules or requirements before being added to NDOT systems.
- NDOT reserves the right to perform regular audits to ensure compliance with data quality validation rules, encryption protocols and MFA implementation, use of standardized data formats and integration methods, mobile device security measures, adherence of cloud service providers to NDOT's standards, and implementation of RBAC.

Related Documents:
NRS 603A, TP 3-11_Data_Governance_Policy, TP 1-3-13 Cloud Services Policy, TP 1-3-15 Mobile Device Policy
Data Governance Policy
NDOT Cloud Services Policy
Mobile Device Policy
State Cloud Services Standard

DATABASE PRODUCTS AND STANDARDS

The DEPARTMENT has established Microsoft SQL-Server as the primary Relational Database Management System (RDBMS).

- All Database management systems (DBMS) must be based on the relational or object-oriented model.
- If DEPARMENT hosted or DEPARTMENT maintained, then we require Azure SQL Database or Microsoft SQL Server 2022. An estimate of the database size and growth rate must be provided prior to implementation.
- The Azure SQL Database time zone is always set to UTC regardless of geographical location. Applications must accommodate local time zone conversions when inserting into and reading from databases.
- Database Authentication and Authorization should use Azure Identity and/or Active Directory. Other types of Authentication and Authorization mechanisms require an ISO security exception approval.
- All database communications must utilize private endpoints. The use of public endpoints requires approval of an exception to this policy.
- Vendors must set up and maintain separate environments for development, test, and production.
- Direct access to production databases or database servers by vendors is strictly prohibited.
- Vendors must provide a contact list of employees providing support to the Department.
- Personally Identifiable Information (PII) data, Protected Health Information (PHI) data, and Payment Card Information (PCI) data must be encrypted in transit and at rest per Nevada Revised Statute (NRS 603A), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974.
- SQL Server database deployments and changes must be scripted.
- Online Transaction Processing (OLTP) databases:
    - Data logic and business rules must be encapsulated.
    - Ad hoc queries and data modifications are strictly prohibited.

- Errors must be handled in procedure code without being passed directly to client applications.
- Revoke or deny all permissions to the underlying tables for all roles and users in the database.

APPLICATION DEVELOPMENT PRODUCTS AND STANDARDS

Application developers and administrators must follow the Software Development Life Cycle (SDLC) process to ensure proper coding and avoid programming deficiencies. The SDLC procedures include fundamentals to ensure security risks do not expose the DEPARTMENT'S data and information systems. Applications for end users should be developed in the web software environment. Application developers should keep in mind that some remote offices and public access users still only have limited internet connectivity. Additional requirements on Web, database, network security, and other IT related issues should be investigated with the IT division.

Applications Developed to be maintained by NDOT IT Staff:

- Software Developed for the DEPARTMENT which will be maintained by NDOT IT Staff must be hosted in the NDOT Azure Tenant.
- Software Developed for the DEPARTMENT must utilize the native tools and features of Azure (Web Apps, Logic Apps, Web Jobs, Functions, Data Factory, etc.) when being developed.
- Software Developed for the DEPARTMENT must be developed using the .NET Core framework at the latest version available at the time of development.
- Web-based Software Developed for the DEPARTMENT must be compatible with, and remain compatible with, the most recent three versions of Microsoft Edge, Chrome, Safari, and Firefox.
- User Interface Theme must utilize the DEPARTMENT's approved skin/theme for the application.
- Use of external code/projects/frameworks must utilize standard Package Management System (Sass, NPM, YARN, GULP etc.).
- All Source code for the project must utilize the NDOT Azure DevOps Environment (GIT Repository) for the main repository.
- Beta software used in projects is strictly prohibited.
- Reporting shall use the DEPARTMENT's standard reporting tools, currently Power BI Government Edition.
- Source Code shall be documented within the source where applicable and necessary to explain the portion of code for later reference.
- Require the use of Swagger (Azure default) or other Interface Description Language for Describing REST endpoints.
- Code Stack, Architecture and Language must be reviewed and approved by the Development Team before development begins. (C#, MVC, Angular are preferred technologies being asked to use but will review other requests as needed for the development project.)
- Database shall use Azure SQL Server or Microsoft SQL Server.
- Database Architecture/Schema must be reviewed and approved by the Development and Database teams before development begins.
- A defined QA/QC Program must be submitted, reviewed, and approved by the QA/QC Team before development begins. (Use of automated testing, manual testing, etc.)

Applications Developed to be maintained and hosted by Vendor:

- Must adhere to the State Cloud Policy
- Must adhere to the NDOT Cloud Policy
- Must use (Microsoft Entra ID) or other approved authentication which will allow Single Sign On Capabilities for NDOT Staff.
- All Data/Programs must be stored in USA servers. No exceptions.
- Interfaces needed by other applications shall be developed using standard API end points.
- Database may be selected by the vendor, and vendors must provide a contact list of employees providing support to the Department. If DEPARMENT hosted or DEPARTMENT maintained, then we require Azure SQL Database or Microsoft SQL Server 2022. An estimate of the database size and growth rate must be provided prior to implementation.
- Coding of application may be selected by the vendor, no preference when maintained/hosted by vendor.
- QA/QC of application shall be documented and provided to QA/QC Team for review and approval.

Any Software developed for NDOT, regardless of who is hosting/maintain the application, must adhere to the following secure coding practices:

- Validate input from all data sources before use.
- Compile code using the highest warning level available for your compiler and eliminate warnings by modifying the code.
- Architect and design for security policies. Create a software architecture and design your software to implement and enforce security policies.
- Keep the design as simple and small as possible.
- Default deny. Base access decisions on permission rather than exclusion.
- Adhere to the principle of least privilege. Every process should execute with the least set of privileges necessary to complete the job. Any elevated permission should be held for a minimum time.
- Sanitize data sent to complex subsystems such as command shells, relational databases, and commercial off-the-shelf (COTS) components.
- Practice defense in depth. Manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense can prevent a security flaw from becoming an exploitable vulnerability and/or limit the consequences of a successful exploit.
- Use effective quality assurance techniques. Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities. Fuzz testing, penetration testing, and source code audits should be incorporated as part of an effective quality assurance program.
- Adopt a secure coding standard. Develop and/or apply a secure coding standard for your target development language and platform.
- Identify and document security requirements early in the development life cycle and make sure that subsequent development artifacts are evaluated for compliance with those requirements.
- Use threat modeling to anticipate the threats to which the software will be subjected. Threat modeling involves identifying key assets, decomposing the application, identifying, and categorizing the threats to each asset or component, rating the threats based on a risk ranking, and then developing threat mitigation strategies that are implemented in designs code, and test cases.

SYSTEM PRODUCTS AND STANDARDS

It is important to maintain the configuration of the DEPARTMENT servers. These servers store, process and transmit critical information.

- Privileged access must be strictly limited. System administrators will control granting access privileges to users in accordance with DEPARTMENT policies. It is our practice to follow "least privilege access" / "just in time access" whenever possible.
- Only DEPARTMENT approved software will be installed on DEPARTMENT workstations, laptops, or servers. To avoid technological incompatibility issues, security exposures, software incompatibility issues, and management issues, non-DEPARTMENT issued or approved software is strictly prohibited.
- All server operating systems need to be current at the time of implementation.
- All servers must be virtualized. (If a physical server is required, an exception to this policy must be approved before implementation.)
- Servers must run within Azure VMware (AVS) or within Microsoft's native Azure environment. If it is not possible for a virtual server to run within an off-site cloud environment, the vendor may request approval to use an on-site VMware environment.

ACTIVE DIRECTORY/DNS STANDARDS

- Azure Managed Identities are preferred where possible. If not possible, group managed service accounts must be used. Exceptions to this standard must be approved by the ISO.
- Separate Admin accounts for administrative tasks are required.
    - FBI fingerprint-based background checks are required for physical access or logical administrative access to all DEPARTMENT servers and workstations by 3rd parties.
- Whenever possible, Azure AD guest accounts must be used for contractors\vendors who do not require an internal NDOT account.
- For enterprise applications a specific security group will be created.
- Outside DNS zones are hosted in Azure and controlled by the NDOT systems team.
- Internal DNS leverages Azure AD\DNS VMs for all "non-authoritative" requests.
- SAML Authentication must use Azure AD.
- Applications should use automatic provisioning of users and groups with Microsoft Entra ID (Formally Azure AD) through SCIM 2.0 or better. Exceptions to this standard must be approved by the ISO.

WEB PRODUCTS AND STANDARDS

The following products and standards should be considered when developing web-based solutions.

- Browser support- Current version plus one previous version:
    - Microsoft Edge (latest version plus two versions); and
    - Firefox (latest version plus two previous versions); and
    - Safari (latest version plus two previous versions); and
    - Chrome (latest version plus two previous versions).

- Applications must be developed using the latest in Responsive Web Techniques (Mobile First Design) to allow for use on various devices including, but not limited to: desktop, mobile, tablets, etc.
- Must follow W3C standards and specifications.
- webDAV usage is not allowed.
- Use of Flash is prohibited.
- Use of Silverlight is prohibited.

GEOGRAPHIC INFORMATION SYSTEMS PRODUCTS AND STANDARDS

The DEPARTMENT is implementing an Enterprise Geographic Information System built upon the Esri software platform and using ArcGIS for Portal, ArcGIS Online, and Esri Roads and Highways.

GIS Software Compatibility

- All routes and event tables must support Esri's Roads and Highways version 10.9.1 or higher. The DEPARTMENT is currently utilizing ArcGIS Server 10.9.1 or newer with SQL Server 2019. Preferably PAAS Azure SQL servers.
- **Vendors doing business with the DEPARTMENT must ensure their products are compatible with the current version. If the DEPARTMENT upgrades to a newer version, vendors are required to ensure compatibility with the new version.**
- Any server-side processes must use ArcGIS Server Geoprocessing services, ArcGIS Web API, Runtime SDK (such as Qt or .Net), Python API, Server Object Extensions (SOE), or Server Object Interceptor (SOI) for ArcGIS Server 10.9.1 or higher. ArcGIS Desktop/Pro or other client-based software cannot be installed on DEPARTMENT servers.

GIS Data and Services

- All spatial data developed and delivered by the vendor must reside on and be actively managed on the DEPARTMENT's Enterprise geodatabase or the Portal for ArcGIS Data Store.
- All data should be delivered as a file geodatabase with database design approved by the DEPARTMENT's business unit or created directly in our existing databases. This includes Geodatabase domains, subtypes, and topologies.
- All Linear Referencing System (LRS) event tables shall be registered with the DEPARTMENT's ArcGIS Roads and Highways which shall reside on the DEPARTMENT's Enterprise Geodatabase.
- DEPARTMENT-owned GIS data used by a web application will be delivered using a Map Service hosted by DEPARTMENT's ArcGIS Server, on the DEPARTMENT's ArcGIS Online site, or on the DEPARTMENT's Portal for ArcGIS site.
- To keep data current and prevent import/export work by staff, GIS data used in a web application will be provided using an NDOT ArcGIS Server map service, Portal hosted feature service, or ArcGIS Online registered feature service. All data will reside on the DEPARTMENT's Enterprise Geodatabase or ArcGIS for Portal Data Store.
- Vendors who deliver any solution(s) based on web services must provide a map document, map package, or layer package that has been approved and finalized by the DEPARTMENT's business unit – including all symbology, display queries, map scales, and labels or annotation prior to deliver to the DEPARTMENT's IT GIS Team for publishing as a map service.
- The addition and removal of fields in any dataset must first be requested through the IT Service Desk to the IT GIS Team. The GIS Data Steward or their approved surrogate will be provided access to the Enterprise Geodatabase in the Development environment to make modifications to new or existing schema. Once complete, the IT GIS Team will move the schema changes to the Enterprise Geodatabase in the Test environment where applications using this data will be confirmed to work without error. Once effective QAQC has been performed, the IT GIS Team will move the schema changes to the Enterprise Geodatabase in the Production Environment. Due to web application and

geoprocessing tool dependencies, vendors do not have permission to add/remove fields or add/remove datasets in the Production environment.

Data Dictionary, Metadata and Data Projections

- The DEPARTMENT requires that all data sets use the UTM NAD83 Zone 11N map projection.
- All geospatial data must be provided with a data dictionary approved by the business unit – including the full names of attributes, meanings of codes, scale of source data, and accuracies of locations.
- All geospatial data must contain Federal Geographic Data Committee (FGDC) metadata within the dataset.

Mobile Data Collection

- Fieldmaps for ArcGIS or Survey123 is required.
- Mobile web applications must be built to support the iOS platform.
- If the DEPARTMENT's business unit is planning to collect data on a GPS unit, please refer to the DEPARTMENT's business unit for hardware requirements.

Mobile Devices using geospatial data must allow offline syncing and disconnected editing for spatial data.

GENERAL SECURITY STANDARDS

- All data in transit must be protected using the TLS 1.2 or newer protocol.
- The DEPARMENT or State data must be encrypted at rest using an encryption method agreed to by the DEPARTMENT. Whenever possible, the DEPARTMENT should control and manage the encryption keys.
- All communication channels between DEPARTMENT systems and non-DEPARTMENT systems which carry sensitive data must use a virtual private network (VPN) connection.
- Self-signed encryption certificates are prohibited. Certificates will need to be signed by a publicly trusted Certificate Authority for the public facing applications. Backend services can be signed by the DEPARTMENT's Internal Certificate Authority.
- Cloud Service Providers (CSP) must meet the Center for Internet Security (CIS) Controls identified as applicable in the current CIS Controls Companion Guide for the service model (Infrastructure as a Service, Platform as a Service, Software as a Service, or Function as a Service) they provide.
- CSP data centers, staff, and contractors collecting, processing, transmitting, storing, or interconnecting the DEPARTMENT's data in a cloud environment must be located within the continental United States.
- Multi-factor Authentication is required.
- Cloud services must enforce least-privilege access to data, based on access roles established or agreed to by the DEPARTMENT.
- Cloud services must use the DEPARTMENT's Microsoft Entra ID tenant as the authentication mechanism for access.