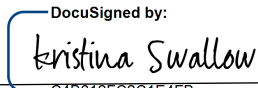


STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

Approved  _____
C4B612FC2C1E4FB...

TECHNOLOGY USE POLICY

1. PURPOSE

To establish policy that outlines the acceptable use of information technology resources for Nevada Department of Transportation. The rules are in place to protect the employees and NDOT from inappropriate use that may expose NDOT to risks including, but not limited to the compromise of network system and services or legal issues.

2. POLICY**Access and Use**

All user access will be requested on a Computer Access Request Form and pre-approved by their Division Chief prior to the account creation. Access will be limited to only information technology resources necessary and appropriate for the user to perform their job functions. Users may use the NDOT information technology resources to:

- a. Further the Agency's mission;
- b. Deliver Agency services;
- c. Facilitate business-related research and access to information;
- d. Provide services of the highest quality to citizens;
- e. Discover new ways to use existing department resources to enhance the Agency's service;
- f. Increase staff efficiency; and
- g. Promote staff development.

Assigned user accounts or credentials are to only be used by the individual to whom they have been assigned. The sharing of accounts is prohibited, except for kiosk accounts.

Users are prohibited from representing themselves as someone else, disguising, or suppressing theirs or another's identity.

Account passwords must not be shared and are required be changed every ninety (90) days, except for service and kiosk accounts which must be changed annually.

Upon termination of employment or contract with NDOT, accounts will be disabled, and the user shall not use or attempt to use any NDOT account, access codes, and privileges.

STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

Users will comply with all copyright laws and contractual agreements relating to the use or reproduction of any information technology material used within the NDOT network.

Personal Use

Information technology resources are to be used for work related assignments and business purposes. Users shall not use information technology resources for:

- a. Political lobbying or campaigning;
- b. Engaging in gambling of any sorts;
- c. Viewing pornographic or sexually explicit content or materials;
- d. Transmission, display or storage of any material that is racist, sexist, threatening, harassing, obscene or otherwise objectionable;
- e. Personal gain or the production of income to any entity or individual other than the Department;
- f. Posting in non-business-related chat rooms or on non-business-related internet web logs (blogs);
- g. Using to illegally make, acquire, use or provide unauthorized copies of any information protected by copyright, including without limitation to music, video, web casts, streaming media, audio content, software, designs, or other intellectual property.

Pursuant to NRS 281A.400 (7), such NDOT information technology resources may be used for limited personal purposes if:

- (1) The use does not interfere with the performance of the employee's public duties;
- (2) Personal use must not affect the performance of the computer network;
- (3) The cost or value related to the use is nominal; and
- (4) The use does not create the appearance of impropriety.

STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

Limited personal electronic files and documents pursuant to the allowance in NRS 281 as described above may be stored on the user's assigned OneDrive Storage. Personal files and data are not allowed to be stored on a network drive or workstation. Network storage is strictly for business related documents only. The Agency is not responsible or liable for any personal electronic files stored on Agency-owned equipment.

Personally owned devices are not allowed to connect to the NDOT network. Additionally, users acknowledge and accept that any work they choose to do on their personal devices is the property of NDOT, subsequently making the entire device subject to legal holds and e-Discovery.

Cloud Services

The use of non-approved Cloud Services is prohibited. Please refer to TP 1-3-13 for approved uses of cloud services.

Electronic Documents

All electronic data, files, documents, and communication created in the performance of an employee's duties at NDOT need to be stored on OneDrive or other Agency designated file storage. Data stored locally on personal computing devices is not backed up and susceptible to data loss. All electronic data, files, documents, and communication created by NDOT staff or contractors during the performance of their duties using NDOT information technology resources are the property of NDOT and are subject to review to fulfill Public Records Request Electronic Discovery (eDiscovery) or court ordered requests or personnel related matters. The information technology staff will collect any and all electronic information and provide it to the authorizing party(s).

Electronic Mail (e-mail)

Users will use the email system to send and receive communication with peers, contractors, customers, partners, and general public in order to carry out their job duties. Users will keep their communications professional and respectful. The following email activities or use are prohibited:

- a. Political lobbying, campaigning, or sending/forwarding political opinions and viewpoints;
- b. Pornographic or sexually explicit content or materials;
- c. Jokes;
- d. Chain letters;

STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

- e. Religious materials, activities or causes, including viewpoints or inspirational messages;
- f. Sending or forwarding email that contain malware or phishing attacks;
- g. Charitable solicitations unless approved by Human Resources;
- h. Materials related to personal ventures or to enhance personal gain;
- i. Posing as anyone other than oneself when sending;
- j. Sending account credentials and/or passwords;
- k. Defaming others by: spreading false allegations or rumors that would harm a person's reputation.

Privacy

Except as otherwise provided by applicable law, users shall not have an expectation of privacy for any information they create, store, send or receive on any NDOT information technology asset.

In accordance with NRS 200.650, a user is prohibited from using information technology assets to surreptitiously video, record, or listen to another person's private conversation or activities without the express consent of the individuals.

In accordance with NRS 281.195, anyone adding, copying, deleting, manipulating or observing the files or other information stored on a computer, whether such actions are carried out directly or remotely of another employee's computer, outside of normal routine Information Technology maintenance, must give them 48 hours' notice either prior to or after the system was accessed.

Removable Media

Electronic media, including portable/mobile media containing confidential, restricted, or sensitive data not in the presence of the authorized user must be secured within a locked environment. Confidential data residing on portable/mobile media must be protected through encryption and password protection.

Users must check all electronic media, such as software, diskettes, CDs and files for viruses when acquired through public networks (e.g., internet sites) or from outside parties by using virus detection programs prior to installation or use. If users suspect a virus, the

STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

applicable system(s) or equipment must not be used until the virus is removed. The matter must be immediately reported to the IT Service Desk.

Security

The use of information technology resources for hacking and other crimes related to computer security is strictly prohibited including but not limited to:

- a. Gaining unauthorized access to a computer system;
- b. Trying to defeat the security features of the IT resources;
- c. Distributing malicious code, viruses or malware with the intent to cause harm;
- d. Interfering with computer systems by damaging or interfering with others' lawful use of data and computers.

The storage and/or transmission of any Personally Identifiable Information (PII), Health Insurance Portability and Account Act (HIPAA), or Payment Card Industry (PCI) data must be encrypted using Information Technology Division approved encryption software or algorithms (see NRS 603A.040). Additional means to secure and control intellectual property and sensitive information must be taken.

All users assigned an NDOT user account must take a minimum of one hour of Information Security Awareness Training annually.

Users that have gone through the annual Internet Security and have clicked one or more phishing attack and/or introduced malware into the network and/or network credentials compromised are subject to disciplinary actions, including written reprimands and/or being required to be enrolled in additional security training as required by the Security Officer.

Social Networking

NDOT Social Media is to be used to represent the Department in an official capacity and communicate official NDOT messages to the public. For acceptable uses of social media, please refer to Transportation Policy 1-1-2 Employee Communications Social Media Policy.

Software

Only Information Technology approved, and properly licensed software will be used or installed on NDOT computers and mobile devices and will be used according to the applicable software license agreement. All software is to be acquired in accordance with NDOT TP 1-3-9.

STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

The downloading of non-approved executable software, such as screen savers, freeware/shareware, demo software or software upgrades are prohibited without the express approval of the IT division.

3. SCOPE

This Transportation Policy (TP) applies to any NDOT employees, independent contractors, consultants, temporary or part-time employees, interns, service providers, partners, and other persons granted access to any part of the NDOT network or technical equipment owned, leased or managed by NDOT.

4. BACKGROUND

Information technology resources are a valuable asset to the Agency and are provided to enhance the core functions of NDOT. The Agency relies on a networked technology system and the data contained within it to fulfill its duties and mission. This policy is in compliance with the STATE OF NEVADA Information Technology Acceptable Use Agreement 103 and the State Information Security Consolidated Policy 100.

5. DEFINITIONS

- a. Information Technology Resources: all technology equipment, hardware, software or network (including wireless) and includes computers, e-mail, applications running on NDOT's or the state's internet or intranet sites including approved cloud service providers.
- b. Personal Identifiable Information (PII): a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:
 - Social security number.
 - Driver's license number or identification card number.
 - Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.
- c. Social Networking: varieties of websites that allow users to share content, post messages, photographs, interact and develop communities around similar interests.

STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

- d. Removable Media: Storage media which is designed to be removed from the computer without powering the computer off. This includes, but is not limited to DVDs, CDs, memory cards, USB flash drives, external hard drives.
- e. User: NDOT employees, independent contractors, consultants, temporary or part time employees, interns, service providers, partners, and other persons whom NDOT has explicitly granted access to NDOT's information technology assets and information.
- f. Electronic Discovery: Electronic Discovery, commonly referred to as eDiscovery, is the collection of electronically stored information (ESI) or information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software during the course of litigation.
- g. Public Records Request: A request for NDOT electronically stored information (ESI) can also be initiated through a public record request pursuant to NRS Chapter 239 requesting the collection of electronically stored information (ESI) or information created, manipulated, communicated, store, and best utilized in digital form, requiring the use of computer hardware and software.
- h. Court Ordered Request: A request for NDOT electronically stored information (ESI) through a subpoena issued by a court.
- i. Cloud Services: Style of computing where scalable and elastic IT-enabled capabilities are provided 'as a service' using Internet Technologies.

6. RESPONSIBILITY

- a. Division Heads and District Engineers are responsible for:
 - (1) Employee compliance with this policy;
 - (2) Notifying NDOT Information Technology Division of the need to terminate access of an employee, contractors prior their termination or immediately upon termination.
- b. Employees, independent contractors, consultants, temporary or part-time employees, interns, service providers, partners, and other persons with access to information technology resources are responsible for:
 - (1) Reviewing and signing the Acceptable Use Agreement form (attached);

STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

- (2) Ensuring the proper use of their account and any actions performed with their user account is the responsibility of that user;
- (3) Following this policy in its entirety as well as all applicable laws pertaining to information technology access, data transmission, etc.;
- (4) Understanding that any information or electronic files stored on or transmitted through any NDOT owned information technology resources is property of NDOT and may be reviewed by NDOT at any time. The same information is available to individuals or entities outside of NDOT should the records be requested through lawful means.

c. Information Technology Division is responsible for

- (1) Initiating, revising, and interpreting this TP; and
- (2) Creating, disabling or deleting of accounts when authorized per this policy.

7. PROCEDURE

a. Computer access request:

- (1) EMPLOYEE'S SUPERVISOR:
 - Completes and signs a Computer Access Request Form
 - Sends it to the IT Service Desk
- (2) SERVICE DESK:
 - Creates a work order
 - Notifies the requester via email the work order has been created
- (3) EMPLOYEE:
 - Sends the signed Acceptable User Policy to Human Resources
- (4) TECHNICIAN:
 - Sets up the employee within 3 business days of receiving either or both signed Computer Access Request Form and Internet Usage and Email Policy Acknowledgement Form.
 - Notifies the requester that the work is complete

STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

- b. Change/Transfer computer access:
- (1) EMPLOYEE'S SUPERVISOR:
 - Completes a Computer Access Request Form
 - Sends it to the IT Service Desk
 - (2) SERVICE DESK:
 - Creates a work order
 - Notifies the requester via e-mail that the work order has been created
 - Changes are made within 3 business days of the work order being created
 - Notifies the requester that the work is complete
- c. Delete/Terminate computer access:
- (1) EMPLOYEE'S SUPERVISOR:
 - Requests that the Service Desk disable the employee's access at the earliest possible time after termination.
 - (2) SERVICE DESK:
 - Creates a work order
 - Disables the employee's access within 30 minutes of being notified
 - Deletes the account (once the official notification of termination has been received)
 - Notifies the supervisor when the work is complete

END

STATE OF NEVADA DEPARTMENT OF TRANSPORTATION

March 13, 2020

TP 1-3-14

Technology Use Agreement & Acknowledgement

This is to certify that I have read and agree to abide by the guidelines set forth within the NDOT Technology Use Policy. As an employee or business partner of NDOT, I fully intend to comply with this policy realizing that I am personally liable for intentional misuse or abuse of the Agency's computer systems or information. If I have any questions about this policy, I understand that I need to ask my supervisor or Information Security Officer (ISO) for clarification.

*If I refuse to sign this acknowledgement form, my supervisor will be asked to sign this form indicating that I have been given time to read and have had questions answered about this agreement. The supervisor will read this statement to me prior to signing the document and advise me that by not signing this document my rights to use the Department's computer systems may be denied and may affect my ability to meet my job requirements.

Name (please print)	
Signature	
Date	

Supervisor Signature	
Supervisor Comments	
Date	