DEPARTMENT OF TRANSPORTATION
POLICY/PROCEDURE

Network Security, Access, and Use	Effective Date: 11/29/2021	Commissioner Approval: Signature on file Lewis Daidone, Assistant Commissioner Finance and Administration Signature on file Contact Telephone #:

I. PURPOSE AND SCOPE

To outline the policy of the NJDOT on the appropriate use, necessary restrictions, and responsibilities of State-provided Network connections and Internet access and use.

Employees shall have no expectation of privacy when accessing and using: State-issued devices/equipment; the GSN used to communicate; and/or the electronic data stored thereon.

This policy applies to all NJDOT employees and system users whether authorized or unauthorized who access and use the Network/Internet, and encompasses all decisions and activities affecting or affected by access or use of the Network/Internet by agency employees and system users whether authorized or unauthorized.

II. DEFINITIONS

Access - as a verb, to gain the ability to view and read the contents of a computer and/or maintained file.

Disclose - to expose a computer-generated and/or maintained file to the attention of someone other than the originator or original recipient.

Garden State Network (GSN) or Network – the New Jersey State data network which allow internal and external communication for New Jersey State employee computers and digital phones.

Internet - the vast collection of inter-connected networks that all use the TCP/IP protocol.

Internet Service Provider (ISP) — an entity that provides access to the Internet.

Information Technology (IT) – unit within the DOT which implements, manages, and supports technology used by the Department.

Management - an NJDOT employee who is a member of executive leadership (Commissioner, Assistant Commissioner, Chief of Staff, Inspector General, Executive Director) and/or other primary level supervisor.

Monitor - as a verb, to check, observe, test, track, log, or watch, whether by computer program or human perception.

Network – servers and telecommunication lines that store, use, and share information.

Network/Internet access - network infrastructure and services that allow for a communication path between workstations, servers, network services, state-hosted applications, and the State Internet Service Provider (ISP) for internet access.

NJDOT owned equipment – any computing, network or electronic data equipment purchased, configured, or maintained by NJDOT or the New Jersey Office of Information Technology.

Other supervisory personnel - NJDOT employees other than management who sign time reports and complete Performance Assessment Review (PAR) forms as part of their job descriptions.

Personal devices – any non-NJDOT supplied hardware lacking the required authorization from the DOT Division of Information Technology, including but not limited to, cell phones, personal computing devices, external storage drives, USBs, or any other device connected to any port or network cable.

Web filter – a monitoring tool that filters websites based on approved access as deemed by DOT Management and used by NJDOT Bureau of Information Security and Services.

III. RESPONSIBILITIES

It is the responsibility of the Division of Information Technology to maintain this policy and ensure it is implemented throughout the Department.

A. NJDOT Network Users

Users of the GSN must comply with this policy.

Users must review and acknowledge that they have read this policy.

Users of the GSN/Internet service must be aware that abuse of the Internet service and related policies may result in disciplinary action based on monitoring information.

B. Manager or Other Supervisory Personnel

Ensure staff adhere to this policy. Report any violations constituting major offenses to Office of Inspector General (OIG), as required by Policy 200 - Investigative Services.

Distribute the policy to all vendors. Obtain written or e-mail confirmation of receipt of this policy.

Actively educate employees on the proper use of the Network/Internet.

Distribute and establish internal controls to enforce this policy.

Upon finding that a reasonable basis of unauthorized employee Internet use exists, request an Internet usage report or other relevant data report from the Director of IT with concurrence from member of executive leadership or designee. If, during monitoring, the Division of IT is made aware of any form of abuse or violations, Human Resources management and/or the Inspector General's office will be notified.

Request revocation of or limitation of network and/or internet access or refer for disciplinary action if an employee or person(s) abuses the Network/Internet system as stated herein.

To request an exception for a single employee, an approved Form IT-16 must be submitted to the Director of Information Technology. The requesting manager must advise IT when an employee no longer requires the requested exception.

To request an exception for an entire unit, an approved Form IT-16A must be submitted to the Director of Information Technology with the appropriate Assistant Commissioner's concurrence. The requesting manager and subsequent managers must inform employees new to the unit of the previously approved exception and not to abuse the level of access granted based on the exception. The requesting manager must advise IT when the unit no longer requires the requested exception.

C. Division of Information Technology

Provide and maintain Internet access.

Routinely monitor access and use of the Network/Internet by NJDOT network users.

Provide a web activity report about a specific employee's or employees' Internet usage when requested by a member of management with approval from a member of executive leadership or their designee; the Division of Human Resources; the Office of the Inspector General; or a law enforcement entity entitled to the information as part of an enforcement action.

D. Division of Human Resources

Ensure that all DOT employees are provided with this policy within 30 days of employment and obtain employee acknowledgement of the contents of this policy on a yearly basis.

Discipline employees for violation of this policy. See Policy 532 – Discipline.

E. Office of the Inspector General

Investigate reported incidents.

Where appropriate, authorize an internal review of an employee's use of network access and internet usage.

Where appropriate, direct the suspension of access and use of during and/or after investigation for the purpose of preserving evidence of an administrative, civil, or criminal investigation.

IV. POLICY AND PROCEDURE

Policy

It is the policy of the NJDOT to encourage the use of the Network or Internet by its employees for business related purposes only. When the Network or Internet is used appropriately it is a cost effective, timely, and efficient tool for assisting employees with meeting the Department's program goals. As such, each employee is responsible to comply with various Statewide Policies on Network and Internet use incorporated herein. The Department expressly prohibits

use of the GSN or Internet for purposes that would be illegal, unrelated to NJDOT business, or cause network infrastructure degradation.

Procedure

1. Monitoring

State-provided Internet use is monitored. Internet usage reports may be generated and provided to management for review. Any significant unauthorized misuse discovered must be reported for possible disciplinary action. The Department allows minimal personal use of its Internet/e-mail system on authorized NJDOT owned equipment only during authorized breaks and/or lunch periods.

Authorized systems administrators, during system maintenance and/or normal operations, shall report any unauthorized use or breaches of security discovered to the appropriate personnel. Any devices including personal devices connected to the Department Network may be seized or impounded only by or at the direction of the NJDOT Inspector General, or a local, state, or federal law enforcement agency.

Approval to access or disclose Network/Internet use (excluding email) is hereby granted by the Commissioner to the members of executive leadership and NJDOT division directors for any legitimate purpose, including disclosure to a Deputy Attorney General, for the purpose of representing the Department's interests in any actual or anticipated civil, administrative, or other legal action in which the Department is or may become a plaintiff or a defendant.

Approval to access or disclose Network/Internet use (excluding email) is hereby granted to the Inspector General or designee, for the purpose of:

- conducting an internal investigation in accordance with Policy 200 – Investigative Procedures;
- directing NJDOT compliance with an external criminal, civil, regulatory, or other investigation;
- conducting an internal audit in accordance with routine NJDOT auditing protocols or as otherwise directed by the Commissioner;
- coordinating an internal audit or performance review conducted by NJDOT OIG Internal Audit or by an external audit coordinated by NJDOT OIG Internal Audit in accordance with Policy 237 - External Audits – Initiation, Control & Response.

2. Correctly Accessing the NJDOT Network

Department employees and other explicitly authorized users may only access the network by using approved services and equipment.

A. Authorized Internet Service Providers (ISP)

Employees must use the State's Internet Service Provider (ISP) which is accessed solely through the Garden State Network (GSN). Employees are prohibited from using other ISPs on NJDOT owned equipment. There may be exceptions made to this policy if special

requirements exist. Exceptions must be requested in writing to the Division of Information Technology for approval.

B. Filtering Software and Exemptions

NJDOT uses a web filter solution to filter websites and to block inappropriate or non-business-related websites. Exceptions to the web filter rules can be provided to employees or business units for business related websites or categories with the approval of a division director or above. To request an exemption an approved Form IT-16 (individual) or Form IT-16A (unit) - Request for Network Policy Exemption must be submitted. The requesting manager must advise IT when an employee or unit no longer requires the requested exception. Also, an employee transferred to another unit within NJDOT will have previously approved web filter exception authorizations revoked upon reporting to the new unit.

C. Permissible Users

Only NJDOT employees, a Deputy Attorney General, and other explicitly authorized persons, such as vendors, (users) may use state-owned equipment. Refer to Policy 356 – Assignment of Desktop and Notebook Computers.

D. Permissible Equipment

Employees are strictly prohibited from using non-NJDOT owned/issued equipment on the Network without prior approval from the Director, Information Technology, or designee. Exceptions must be requested in writing to the Division of Information Technology for approval prior to use of or connection to the network.

Non-NJDOT owned/issued equipment must not be connected until an approved exemption is received in writing. Examples of equipment includes, but is not limited to, computing devices, storage devices, memory cards, thumb or USB drives, wi-fi enabled devices, and/or devices that store, process, or transmit data.

Only State-issued phones may be plugged into a State-issued computer and/or a phone charger but must not be plugged into any non-State-issued computer for any reason, including but not limited to, transfer of data or charging of the device. No exceptions are authorized.

Non-State-issued phones are strictly prohibited from being plugged into a State-issued computer for any reason, including but not limited to, transfer of data or charging of the device; no exceptions are authorized.

3. Permissible Network/Internet Use

The NJDOT promotes the use of the Internet by its employees to improve their productivity. Examples of acceptable Network/Internet use include but are not limited to:

- research related to the employee or network user's State job duties;
- obtaining technical documents/files to perform job functions;
- accessing vendor websites to conduct State business, such as purchasing office supplies;

- communicating with outside agencies; and/or
- providing information to public and private entities as approved by management through the use of approved State of NJ software.

The nature of the Internet itself is non-restrictive; therefore, employees could misuse the Internet. It is easy for employees to become engaged in browsing the web and spending time on non-business-related websites. This is the most common misuse of the Internet by employees. All employees must be mindful of their job responsibilities and only use the Internet to help them perform their jobs with their management's approval.

Limited incidental use is permitted. Filtering software provides a time quota for non-business-related activities, but limits sites to those determined to not be a security risk.

4. Revocation of Network Access

A. Revocation for Cause

Access may be revoked by management with a title of Manager or above if an employee or person(s) violates this policy. Access may be suspended, limited, or permanently revoked and/or disciplinary action may be taken.

B. Revocation Pending Investigation

Access may be revoked at the direction of the Office of the Inspector General, pending the outcome of an investigation.

C. Revocation Upon Separation

Access to the GSN will be revoked upon employee separation from the Department. Unit management is responsible for completing all pertinent forms and adhering to Policy 503 – Employee Separation, which amongst other forms, requires completing Form IT-9 to revoke all network access effective on the employee's separation date.

D. Revocation of Web Filter Exemption Upon Employee Transfer within DOT

Revocation of all web filter exemptions previously approved for the employee will made effective upon the employee's transfer to another unit within DOT. If an exemption is required within the receiving DOT unit, a new Form IT-16 will need to be submitted.

V. AUTHORITY

18 U.S.C. 2510-2523
18 U.S.C. 2701-2713
18 U.S.C. 2721-2725

N.J.S.A. 2A:156-A-1 (NJ Wiretapping and Electronic Surveillance Control Act)
N.J.S.A. 52:18A-224 et seq. (Office of Information Technology Reorganization Act)

Executive Branch of NJ Statewide Information Security Manual

State of New Jersey Technology Circular 18-02-NJOIT

Policy 200 – Investigative Procedure

Policy 356 – Assignment of Desktop and Notebook Computers

Policy 503 – Employee Separation

Policy 532 - Discipline