EXECUTIVE MEMORANDUM

TO:	ALL MDOT STATE HIGHWAY ADMINISTRATION
FROM:	DEPUTY ADMINISTRATOR FOR ADMINISTRATION, LISA B. CONNERS
SUBJECT:	MDOT INTERNET AND EMAIL USAGE POLICY
DATE:	JULY 22, 2019
RESPONSE REQUESTED BY:	N/A

PURPOSE OF MEMORANDUM

To update you on the Maryland Department of Transportation Internet and Email Usage Policy.

SUMMARY

On May 24, 2016, Secretary Pete K. Rahn signed the MDOT Internet and Email Usage Policy. To view the MDOT Internet and Email Usage Policy click here http://mdotpolicymanualinternal/mediawiki/index.php?title=MDOT_276_Email_and_Internet_Usage_Policy. This policy is applicable to all MDOT employees and contractors and supersedes any Transportation Business Unit (TBU) procedure or process related to email and internet use. This policy rescinds all previous MDOT policies, procedures, and manuals. This policy supersedes any previous policies received and acknowledged by employees regarding email and internet usage.

The MDOT Internet and Email Usage policy aligns with Maryland's new IT Security Policy, released by Governor Hogan on June 28, 2019. To view the IT Security Policy click here https://doit.maryland.gov/Pages/press-release07012019.aspx.

MDOT INTERNET and EMAIL USAGE POLICY STATEMENT

1. The Department of Information Technology's (DoIT) State of Maryland Information Security Policy is the official policy in effect for all State of Maryland executive branch employees, including MDOT. The internet and email usage provisions within this policy, and any future amendments, are hereby expressly adopted as MDOT policy and apply to any use of email or internet by users.
2. Consistent with Executive Order 01.01.2015.08 and other applicable State employment rules, users shall protect and conserve State property when using the internet and email and not use State equipment or resources for unauthorized activities.
3. Authorization to access the internet and email is provided to users so that they can efficiently and effectively perform their job duties. Improper or inappropriate use could lead to disciplinary action up to and including termination.

cc: Laurie L. Goudy, Director Office of Information Technology

STATE OF MARYLAND
MARYLAND DEPARTMENT OF TRANSPORTATION
OFFICE OF TRANSPORTATION TECHNOLOGY SERVICES

DIRECTIVE: 1

ELECTRONIC MAIL (EMAIL) AND INTERNET USE BY MDOT EMPLOYEES

1. Introduction

A. The Internet assists State agencies in improving the way they conduct business by providing a quick and cost-effective means to create, transmit, and respond to information electronically. Well-designed and properly managed systems expedite business communications, reduce paperwork, and automate routine office tasks, thereby increasing productivity and reducing costs. Effective management includes filtering spam, monitoring computer use, training, and enforcing information technology (IT) policies with disciplinary actions.

B. Such open access is a privilege and requires responsible use. Users must know and respect the rights of others, respect the integrity of the systems and related equipment, and comply with all applicable laws, regulations, policies, directives, and contractual obligations. Security of this capability is a team effort involving the participation and support of all users who deal with these information systems.

2. Scope

A. This policy applies to the Maryland Department of Transportation (MDOT), including The Secretary's Office and all MDOT Transportation Business Units.

B. Included under this policy are:

1) all users of MDOT and/or State systems, all MDOT employees whether full-time, temporary, contractual, emergency, seasonal, contingency or otherwise, student interns, volunteers, and all MDOT contractors and sub-contractors when accessing the defined networks from State office, offsite, or home locations. The MDOT data network is defined as the MDOT enterprise wide area network (WAN) and associated local area networks (LANs);
2) all Internet and MDOT network activity, including MDOT and State intranets and extranets, that is, private networks that use Internet protocols and the telecommunication system to securely share information;
3) all email activity using MDOT and/or State systems and Internet or non-Internet transport media;
4) all email and Internet records in the possession of MDOT employees or other users of electronic mail services provided by the MDOT data network: and
5) all electronic media, including but not limited to, floppy disks, CDs, DVDs, USB devices, portable hard drives, and optical hard drives.

3. Ownership

Email accounts, files, images, data, and all messages or any other type of electronic communications that are created, sent, printed, copied, or received using the MDOT data network, including from any equipment used

offsite or at home locations, are the property of MDOT. MDOT cannot guarantee the confidentiality of information stored on any network device that is the property of MDOT. Users should have no expectation of privacy in regards to any email, file, data, image or message created, sent, retrieved or received when using MDOT equipment or network access. Authorized network administrators and/or data security employees may access, examine and disclose email, files, images, data, messages, and Internet sites accessed to authorized supervisory personnel the contents of all messages created, printed, sent, or received.

4. Appropriate Use

A. Use of the MDOT data network, email system, and Internet systems are governed by policies that apply to the use of all State property. Use of these resources must be authorized and appropriate. Appropriate use of email and the Internet consists of activities necessary to support the purpose, goals, and mission of MDOT/MdTA and each user's authorized job function. The following conditions apply:

1) **Purpose.** IT resources are provided to conduct MDOT business and to support the MDOT mission.
2) **Restrictions**. Agency services may not be used for unlawful activities, commercial purposes not under the auspices of MDOT, personal financial gain, uses that violate federal or State law, regulations, policies, directives, or for the uses described in 5 of this policy.
3) **Representation**. Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of MDOT or any unit of the State unless authorized explicitly or implicitly to do so. In cases where it appears that the user is representing, giving opinions, or making statements on behalf of MDOT, or any unit of the State, and that user is not authorized to do so, the user shall clearly state that he/she does not represent MDOT or the State.
4) **Information Protection**. Users are responsible for protecting any information used on, or stored in, their accounts, or in their Local Area Network folder such as personal passwords except as required by users' supervisors.
5) **Email Spam Protection**. MDOT makes a best effort to filter spam at the network perimeter to protect network resources from abuse. Users may individually manage suspected spam messages that have been quarantined. They may release messages, delete messages, or request that an address or domain be globally permitted or denied.
6) **Business Use**. MDOT provided network and computer systems that allow or provide access to the Internet and the email system are the property of MDOT and are provided to facilitate the effective and efficient conduct of State business. MDOT permits access to the Internet and email systems to assist in the performance of users' jobs.
7) **Personal Use**. Personal use means use that is not job-related. Incidental and occasional personal use of MDOT's Internet access or email system is permitted; however, personal use is prohibited if it:
    a) interferes with the user's productivity or work performance, or with any other employee's productivity or work performance;
    b) adversely affects the efficient operation of the network; or
    c) violates any provision of this policy, federal or State law, regulation, policy, or directive.

B. Users employing MDOT's Internet or email system for personal use must present their communications in such a way as to be clear that the communication is personal and is not a communication of MDOT or the State. The term personal in this context does not mean private. No user should have any expectation of privacy in any message, file, image, or data created, sent, retrieved, or received by use of MDOT's equipment and/or access. (see section 3)

5. Inappropriate Uses

A. Use of IT resources that does not comply with federal or State laws, regulations, policies, or directives, including laws requiring non-discriminatory and non-harassing communication, and standards of professional conduct is inappropriate. MDOT maintains discretion to determine what is inappropriate use, however, the following list provides examples of inappropriate uses of IT resources.

1) Unauthorized disclosure of confidential, privileged, or proprietary information;
2) Except to the extent required in conjunction with a bona fide, MDOT-approved research project, investigation, or other MDOT-approved undertaking, no one shall utilize MDOT -owned or leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content. "Sexually explicit content" includes, but is not limited to, any description of or any picture, photograph, drawing, motion picture footage, digital image or similar visual representation depicting sexual activities such as sexual bestiality, a lewd exhibition of nudity, sexual excitement, sexual conduct or sadomasochistic abuse or fetishism;
3) Gambling;
4) Engaging in any unlawful conduct, including communications that violate any laws or regulations, including copyright, patent protection, license agreements, or other intellectual property rights of others;
5) Downloading, displaying, sending, or printing threatening, obscene, intimidating, defamatory, fraudulent, discriminatory, harassing or otherwise unlawful messages or images;
6) Use for any purpose that is contrary to State or MDOT policy or the State's best interest;
7) Gaining or attempting to gain unauthorized access to any information facility, including running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords, and electronic eavesdropping on communications facilities;
8) Misrepresenting in any manner an identity, account or computer in an email or other electronic communication;
9) Conducting or soliciting private or personal for-profit or charitable activities, such as consulting for pay or sale of goods, except as authorized by the Secretary or MDOT Administrator/Executive Secretary or designee, such as management sanctioned employee events;
10) Disclosing the name, title, specific illness or home or hospital address of a sick, disabled or deceased employee or family member in a mass distribution email;
11) Sending email using another's identity, an assumed name, or anonymously;
12) Sending email containing Personally Identifiable Information (PII) including but not limited to social security number, driver's license soundex number, credit card number, bank account number (Employees or contractors that inadvertently send or receive email/instant messaging (IM) or CHAT with PII data are required to immediately report it to their manager and/or TBU IT Lead).
13) Permitting others to use an email account for sending unauthorized messages;
14) Personal use that interferes with the user's productivity or work performance or with any other users' productivity or work performance;
15) Bypassing software meant to prevent access to certain websites.

B. There are also inappropriate uses of IT resources, which affect the secure and efficient operation of the network. The following list provides examples of this type of inappropriate uses of IT resources:

1) Listening to radio, television, web cast, and other types of broadcasts, that are not job-related and do not have supervisory approval;
2) Downloading or installing peer to peer file-sharing programs;
3) Downloading or installing games or playing games over the Internet;
4) Downloading or installing screen savers;
5) Knowingly sharing a personal account except where authorized by the Secretary or MDOT Administrator/Executive Secretary or designee, and only when following acceptable security procedures, such as proxy rights;
6) Interfering with or disrupting network users, services, or equipment, including:

    a) distribution of unsolicited advertising or messages;
    b) sending mass mailings to individuals who have not expressly agreed to be contacted, including chain letters and leave donation requests;
    c) propagation of programs intended to damage or overload a computer system by computer worms, Trojan horses, or viruses;
    d) using the network to gain unauthorized entry to another machine on the network.

7) Connecting a Wireless Access Point to the MDOT data network without prior approval from the Change Advisory Board (CAB) approval process;
8) Connecting a non-MDOT laptop to the MDOT data network without prior approval from the appropriate MDOT LAN Administrator;
9) Enabling a Virtual Private Network (VPN) connection to a Third Party network without prior approval through the Change Request approval process;
10) Installing or downloading computer software (either licensed or free), programs, or executable files without permission;
11) Personal use that adversely affects the efficient operation of the computer system, including use of email that could reasonably be expected to cause excessive strain on any computing facilities, such as chain letters, "spam" that exploits list servers or similar broadcast systems to amplify the distribution of unsolicited email, "letter bombs" that resend the same email repeatedly to one or more recipients, and viruses, Trojan horses, and similar agents intended to damage system resources.

C. Users must use reasonable judgment in the performance of their duties and failure to do so may subject them to discipline or loss of IT privileges. Activities on the Internet and email will not be considered misuse when authorized by appropriate MDOT officials for security, performance testing, or document preservation or production for litigation or for Maryland Public Information Act requests.

6. Monitoring

A. MDOT management or designees may track and monitor MDOT record accesses, system usage, web site hits, and emails. This capability helps ensure compliance with the laws, regulations, policies, directives, and standards presented and referenced in this policy. This capability also provides documentation or evidence for analyses or investigations that result from violations of this policy.

B. No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of MDOT's equipment and/or access. MDOT has the right to monitor any and all aspects of its computer systems including sites, instant messaging systems, chat groups, or news groups visited by users, material downloaded or up loaded by users, and email sent or received on

MDOT IT resources. Such monitoring may occur at any time, without notice, and without the user's knowledge or permission.

C. It is the goal of MDOT to eliminate inappropriate use of the Internet. A program is in effect which can review and analyze Internet use by randomly selected users. The program may also monitor Internet use by individuals at management's discretion.

D. Electronic records may be subject to federal Freedom of Information Act or Maryland Public Information Act requests, court orders, discovery related to litigation, or other federal or State laws; therefore such records are available for public distribution or legal proceedings.

7. Consequences of Internet and Email Misuse

A. When misuse of computing, networking, or information resources is suspected, MDOT and immediate supervisors have the authority to direct restriction of email and the Internet, and System Administrators have the authority to temporarily restrict email and Internet privileges under emergency circumstances or in time-dependent and critical operational circumstances.

B. Disciplinary action, up to and including termination, may be imposed for misuse of email and Internet privileges, in accordance with the applicable law, regulations, directives, policies, and procedures. MDOT also has the responsibility to advise appropriate legal officials of any violations, and, if appropriate, institute legal action against violators of this policy, including civil and criminal actions, fines, and incarceration.

C. Reasonable suspicion of inappropriate use of State resources by users may originate from a number of sources including, but not limited to, executives, managers, supervisors, co-workers, the Office of the Attorney General, auditors, criminal investigators, and network monitoring programs. Regardless of how the suspicion arises, the user's Administrator, Executive Secretary, or designee will be notified. That individual will evaluate the strength of the evidence and the seriousness of inappropriate use and decide whether further investigation is warranted. The Administrator/Executive Secretary/designee may direct the MDOT Chief Information Security Officer (CISO) to conduct an investigation. The CISO will use due diligence to ensure that an inappropriate use was performed by the authorized user of the personal computer or other network device in question and not by someone else. The results will be handled as confidential personnel information with written and electronic files stored in secure areas. The results will be turned over to the Administrator/Executive Secretary/designee in a sealed envelope. That individual, with input from the MDOT Human Resources Director and Attorney General, as appropriate, will decide what, if any, disciplinary action will be taken.

D. MDOT recognizes that inadvertent misuse of the Internet may occur when a user is performing functions of the job. MDOT users shall report such inadvertent misuse to ensure a record of the inadvertent misuse is maintained and to protect users from undeserved disciplinary action. A user shall immediately call the MDOT Service Desk at 410-768-7181 or email OTTS_HELPMAIL and provide the user ID, time, date, and site of the inadvertent misuse. The Service Desk will log the call and assign a ticket number. The Service Desk will route the ticket to the MDOT Office of IT Security for review. It is not necessary to report the situation where a user is prevented from going to an inappropriate site by the system and receives the warning that accompanies such prevention.

8. User Acknowledgement

All users must read, acknowledge receipt of and intention to comply with this policy. Users will further acknowledge that the Policy for Electronic Mail (Email), Internet, and Network Use by MDOT Employees may be revised as necessary and agree to comply with current and subsequent revisions of the policy provided to them by MDOT. This acknowledgement shall be made by all users by signing the MDOT Security Policy Acknowledgment Form, prior to their being granted Internet, email, and other network use access from MDOT resources.