ACCEPTABLE USE POLICY (AUP)

NCDOT POLICY C.02.0103

Business Category: Information Technology (IT)	**Business Area:** Information Security Office	
Approval Date: 6/22/2012	**Last Revision Date:** 1/31/2018	**Next Review Date:** 1/31/2020
Authority: N/A **Select all that apply:** ☒ N/A ☐ Requires Board approval ☐ Requires FHWA approval ☐ Requires other external agency approval: Click here to enter external agency name(s).		**Policy Owner:** Information Security Office

Definitions:

Computing system – Computing system is defined as all computers, peripheral devices, information systems, networks, email, and other information technology resources owned, operated on-behalf of, leased by, or controlled by the Department. This includes but is not limited to computing devices that use the Department's network(s) for connectivity. Users shall adhere to all other applicable policies when using other non-NCDOT computing resources.

Policy: This policy defines acceptable use responsibilities when using the North Carolina Department of Transportation ("**NCDOT**" or "**Department"**) computing systems. This policy includes an agreement form that must be signed by each User certifying that the User has read, understands and agrees to comply with this policy.

Many Users are given access to computing systems by the Department. Users shall use Department computing systems for State Government purposes. Users may use Department computing systems for limited personal use so long as that use does not interfere with their work and results in no incremental cost to the Department. The intent of this policy is to ensure proper behavior when using these computing systems. All users shall report suspected or confirmed breaches or loss of any sensitive data (e.g. Highly Restricted, Restricted) or any security incident ***within one hour*** of discovering the incident to the Information Security Office.

Examples of Department computing resources include but are not limited to: computers and related peripheral equipment, software, library resources, telephones (including cellular), facsimile machines, photocopiers, office supplies, network connectivity, mobile devices, instant messaging, and access to Internet services, and email.

This policy in no way limits the use of the Department computing systems for official and authorized activities. The manager is responsible for maintaining a signed copy of this policy for all Users.

Users shall adhere to Statewide Information Security Manual and NCDOT security policies. Users shall retain information in accordance with the General Schedule for State Agency Records and with the NCDOT records retention schedules.

1 Acceptable Use

Users shall not use Department computing systems for activities that are unacceptable. Any devices attaching to, accessing or using Department computing systems (e.g. wired, wireless networks, storage devices such as USB flash drives) must be pre-approved by the Department's Chief Information Officer (CIO). Software shall not be installed on Department computers without prior approval by the CIO. Any device connected to a computing system must meet all

security standards set by the Statewide Information Security Manual and the Department. Misuse or unacceptable use of Department computing systems includes, but is not limited to:

1.1 Any use that causes congestion, delay, or disruption of service to any Department computing system. For example: video, sound or other large file attachments can degrade the performance of the entire network.

1.2 Using Department computing systems to gain or attempt to gain unauthorized access to other systems

1.3 The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter

1.4 Using Department computing systems for activities that are illegal, inappropriate, or offensive - Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

1.5 Using Department computing systems for the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials

1.6 Using Department computing systems for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services)

1.7 Using Department computing systems to engage in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity

1.8 Posting the Department's information to external news groups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a State Government User (unless appropriate Departmental approval has been obtained from the Communication Office) or uses that do not meet the Department's mission or positions (e.g. Social Media Policy)

1.9 Any use that could generate more than minimal additional expense to the Department

1.10 Sending any Restricted or Highly Restricted data, including PII, over email without proper security (e.g. encryption) as defined in the Statewide Information Security Manual or the Department's security policies (e.g. Data Classification and Handling Policy)

1.11 The unauthorized acquisition, use, reproduction, transmission, distribution or installation of any controlled information including computer software, data and ID's, that includes privacy information, copyrighted, trade-marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data (e.g. Software Key Crackers or other software used to circumvent intellectual property rights)

1.12 Installation on the Department's computing systems of any unapproved software

2 Computer Viruses/Malicious Software

It is the responsibility of Users to help prevent the introduction or spread of malicious software. Department computing systems are equipped with a security software (e.g. anti-virus, firewalls, host intrusion detection) and configured to protect the Department's information. The software and the configuration of computing systems are used to protect the Department's information from malicious software and intrusion attempts. In some cases it is used to automatically identify and disinfect malicious software. While using the Department's computing systems, Users:

2.1 Shall not remove or change the configuration of security software (including but not limited to anti-virus, access controls, configuration settings) installed on Department computers.

2.2 Shall report any failure, out-of-date warning, or absence of security software (including but not limited to anti-virus) to the NCDOT IT Help Desk.

2.3 Shall report all malicious software that the security software fails to detect or disinfect to the NCDOT IT Help Desk.

3 Access Management

Users have no inherent right to use the Department's computing systems, software, email, or Internet services. All credentials (*e.g.* username, passwords), personal identification numbers (PIN's), or tokens, regardless of the associated hardware platform, are considered to be state property that has been issued to the User.

3.1 Users shall be responsible for the use of their credentials and for any hardware or software devices and applications associated with their credentials.

3.2 Computer credentials shall be assigned to individuals. The individual is accountable for all activity carried out with their credentials.

3.3 Users shall NOT share their credentials with other users or borrow a credential from someone else.

3.4 All Users shall be responsible for choosing passwords that are difficult to guess and compliant with Statewide and NCDOT Security Standards.

3.5 Passwords shall be kept secret and not revealed to anyone. NCDOT Help Desk will NEVER ask for your password.

4 Security Policy

Users are responsible for familiarizing themselves with the Statewide Information Security Manual and NCDOT Information Security Program and complying with these policies and standards. These policies include the proper classification, labeling, and handling of information as defined by the Data Classification and Handling Policy.

5 Consent to Monitoring

Users DO NOT have a right, nor should they have any expectation, of privacy while using any Department computing system at any time, including accessing the Internet, and using email. To the extent that Users wish that their private activities remain private, they shall not use the Department's computing systems such as their computer, the Internet, or email. By using the Department's computing systems, Users consent to disclosing the contents of any files or information maintained or sent through the Department's computing systems, including location based tracking of assets (e.g. GPS, A-GPS, 3G, or other location aware services). If computer equipment resides in a User's office, cubicle, or workstation, the User acknowledges and agrees that the Department can enter that office/cubicle/workstation to remove the equipment.

By using the Department's computing systems, Users consent to monitoring and recording of their activities, including, but not limited to, accessing the Internet and using email. Use of computing systems is collected through a variety of programs and/or applications. Many systems generate an audit trail. Any use of the Department's communications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

5.1 The Department uses electronic auditing of Users' activities as deemed appropriate.

5.2 The Department applies filters and monitors data processing activities as needed to secure and protect the availability of NCDOT services for employees, contractors, third parties and other Users.

5.3 The Department investigates reported incidents of suspected abusive and/or illegal activities. Investigations of specific individuals are performed in accordance with Office of State Personnel regulations and the Office of Inspector General procedures. The investigations may include reviews of electronic data files and records.

The Department employs monitoring tools to detect improper use. Electronic communications may be disclosed within the Department to Users who have a need to know in the performance of their duties. Information concerning electronic activities by Department users is subject to both internal and external audits. The Department will periodically audit, inspect, and/or monitor the Users' computer and Internet activities. The failure of the Department, Office of State Auditor (OSA), Information Technology Services (ITS), and others to monitor use is not a waiver of their rights to monitor.

All users of the Departments computing systems are advised that their use of these systems may be subject to

monitoring and filtering. By using the Department's computing systems, Users consent to monitoring and recording. The Department has the right to monitor – randomly and/or systematically – the use of Internet and the Department's computing system's connections and traffic. Any activity conducted using the Department's computing systems (including but not limited to computers, networks, mobile devices, email, etc.) may be monitored, logged, recorded, filtered, archived, or used for any other purposes, pursuant to applicable Departmental policies and State and Federal laws or rules. The Department reserves the right to perform these actions without specific notice to the User.

6 Personal Use

Personal use is a privilege, not a right, and may be taken away at any time. This policy does not create the right to use Department computing systems for non-State Government purposes. Nor does the privilege extend to modifying such computing systems, including loading personal software or making configuration changes.

7 Enforcement

Failure of the Department's Users to comply with this Acceptable Use Policy and Information Security Policies and Standards set forth by the State and the Department may result in disciplinary actions up to and including termination of employment. Any unauthorized intentional or as a result of negligence disclosure of information shall constitute grossly inefficient job performance. A violation of the Acceptable Use Policy that results in serious loss of or damage to state property or funds which adversely impacts the state, agency or the business unit constitutes grossly inefficient job performance.

Failure of the Department's contractors to comply with Acceptable Use Policy or other Security Policies and Standards may result in termination of their contract.

The Department may also pursue or may assist other parties in pursuing legal remedies for violations of law or for recovery of damages resulting from violation of information security policies and standards.

8 Deviation Handling

The Secretary of Transportation or his/her designee shall have authority to interpret and apply this policy. The Secretary of Transportation may modify or amend this policy at any time. Requests to deviate from the Statewide and NCDOT Information Security policies and standards should be submitted to the approval authorities designated in the policies and standards. Exceptions shall be permitted only upon receipt of written approval by the Secretary of Transportation.

The Chief Information Officer (CIO) shall direct inappropriate use to the Office of Inspector General for investigation and to Human Resources for appropriate disciplinary action. The CIO may choose to remove access to selected computing systems in order to preserve the integrity, availability, or confidentiality of computing systems under his/her management.

Any actions that are in violation of law will be reported to the Secretary for referral to appropriate law enforcement. These include, but are not limited to:

8.1 18 USC Sec. 1030 - Fraud and related activity in connection with computers

8.2 NCGS § 114-15.1 - Report possible violations of criminal statutes involving misuse of State property

8.3 NCGS Article 60 – Computer/ Related Crime

8.4 17 USC – Copyright Infringement and Remedies

9 Review

The Acceptable Use Policy shall be reviewed at least annually or upon significant changes in the operating or business environment to assess its adequacy and appropriateness. A formal report comprising the results and any recommendations shall be submitted to the CIO.

Scope: The Acceptable Use Policy applies to all fulltime, part-time, and temporary Department employees, contractors, and others employed by third parties ("**User**" or **"Users"**) who perform work on NCDOT premises, or anyone granted access to Department computing systems.

Information regarding the Department's Acceptable Use Policy must be made available to all Users by the Department manager or supervisor responsible for the performance of that User. This policy supersedes any/all previous policies related to acceptable use of computing systems by Users.

Procedures: N/A

Related Documents:

Users are responsible reviewing and understanding the Statewide Information Security Manual and NCDOT Information Security Program and complying with these policies and standards.

- Data Classification and Handling Policy
- Statewide Information Security Manual
- NCDOT Security Policies and Standards
- NCDCR Record retention schedules
- Social Media Policy

NIST Special Publication 800-53 (Rev. 4)

- AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
- CM-11 USER-INSTALLED SOFTWARE
- PS-6 ACCESS AGREEMENTS
- PS-8 PERSONNEL SANCTIONS

Revision History		
Revision Date	**Revision Number**	**Description**
06/22/2012	Version 1.0	New Policy Issued
10/02/2013	Version 1.1	Added Incident Reporting Requirements for SSA
10/21/2014	Version 2.0	Changed Links and References to "Data and System Classification Policy" to "Data Classification Policy"
05/11/2016	Version 2.1	Revised by Carlos Melchiade. No Changes
06/06/2016	Version 2.2	Zimbalist Walker updated hyperlinks
08/18/2016	Version 2.3	Zimbalist Walker removed "Supervisor's Signature"
01/31/2018	Version 4.0	Revised by Barry Knuth. Annual Review; Added relevant NIST 800-53R4 framework control families.

Old Policy	New Policy
Statement of Understanding Regarding Use of Computers and Information Technology Resources by Department of Transportation Employees	Acceptable Use Policy
The Internet and E-mail Policy and Procedures	Acceptable Use Policy