NORTHERN VIRGINIA TRANSPORTATION AUTHORITY

Policy Number 22 – Computer and Electronic Systems Use

I. Purpose. This policy provides guidance with respect to computers, peripherals and other electronic systems.

II. General. The Northern Virginia Transportation Authority (NVTA) computers, peripherals and electronic communications are, as a general rule, to be used only for NVTA related work. Incidental and occasional personal use is permitted. Staff using the Internet represent the NVTA and shall not use it for purposes that are illegal, unethical and potentially harmful to the NVTA and its reputation. Under no circumstances may NVTA computers or other electronic means be used to access pornographic materials, gamble or play computer games. The NVTA computers are Authority property and may be accessed/inspected by the NVTA at any time, without notice to or approval by the employee using the computer.

III. Applicability. The guidance in this SOP applies to all NVTA employees (full or part-time), volunteers or others who may be given permission to use an NVTA-owned or leased computer or other electronic communications.

IV. Expectation of Privacy. All computer, electronic, and telephonic documents and communications (e.g., email, Internet, voicemail, etc.) transmitted by, received by, or stored in the NVTA's networks or computers are the property of the NVTA. Employee use may be monitored at any time to ensure compliance with NVTA policies and SOPs. Any data stored, created or received while using the NVTA's computers or networks are neither private nor confidential. The NVTA reserves the right to access and disclose any of this data, with or without knowledge of the employee.

V. Access to Files and Email. Electronic files and email may be accessed only with the authorization of the Executive Director or the Chief Financial Officer (CFO). The NVTA may also disclose electronic files and email pursuant to a proper discovery request, court order or applicable law.

VI. Prohibited Uses of Electronic Communications. The NVTA prohibits the use of any means of electronic communications that is intended to:

- Harass or threaten other users or interfere with their access to computing facilities.
- Send or forward racially, sexually or ethnically offensive messages.
- Send material that is slanderous or libelous or that involves defamation of character.
- Send fraudulent email.
- Break into another user's computer or mailbox.
- Promote a personal, social, religious or political cause, regardless of worthiness.
- Search for or use websites that involve hate groups or racially offensive or sexually explicit material.
- Gamble.
- Send malicious programs such as computer viruses.

- Participate in activities that promote computer crime or misuse, including but not limited to, posting or disclosing passwords, credit card and other account numbers (other than in legitimate conduct of the NVTA business) and system vulnerabilities.
- Violate any software licensing agreement, to include distributing software.
- Infringe on any copyright or other intellectual property right.
- Send mass mailings of a non-business nature.
- Initiate or forward emails of a non-business nature (e.g., jokes).
- Participate in chain letters.
- Disclose confidential NVTA business information.
- Download and execute any program, screensaver or audio files from the Internet that are not relevant to NVTA business.
- Knowingly introduce a computer virus into the NVTA computers or networks.
- Load diskettes, cd-rom's, dvd discs, flash drives or external drives **of unknown origin** that have not been checked by the CFO or Executive Director.
- Download and use Instant Messaging software.

VII. Access Codes and Passwords. The confidentiality and integrity of data stored on the NVTA's computer systems and networks must be protected by access controls to ensure that only authorized employees and others designated by the NVTA have access. This access should be relevant to employee's or volunteer's job duties. Passwords for employee computers must be changed every three (3) months.

VIII. Physical Security. All computer hardware, software, data and documentation must be secured to prevent misuse, theft, unauthorized access and environmental hazards.

IX. Responsibilities.

A. Chief Financial Officer (CFO).
1. Authorizing access to equipment and files.
2. Authorizing any changes of physical equipment, including purchase and upgrade.
3. Informing Executive Director of any unique or special circumstances.

B. NVTA Clerk.
1. Providing computers and access codes to employees, interns and volunteers.
2. Maintaining inventory of all computer and computer related equipment/software.
3. Authorizing program/application additions or updates for any NVTA equipment.
4. Orienting new employees on this guidance and obtaining agreement below; maintaining record of written agreements.
5. Ensuring that all employees, interns and volunteers are cognizant of this policy and enforcing it.

C. All employees and volunteers/interns using electronic equipment. Compliance with this policy and reflecting understanding of it by signature below.

Approved by the Finance Committee: December 5, 2014
Approved by Northern Virginia Transportation Authority: December 11, 2014

NORTHERN VIRGINIA TRANSPORTATION AUTHORITY

Policy Number 22 – Computer and Electronic Systems Use

Employee/User Agreement

I have read and understand Policy 22 – Computer and Electronic Systems Use and will abide by it.

_____	_____	_____
Printed Name	Signature	Date