Northern Virginia Cigarette Tax Board

Information Technology Administrative Regulations

INTERNET AND TECHNOLOGY USAGE

I. PURPOSE

This purpose of this policy is to define proper usage of technology, including computers, desktops, laptops, cellular phone, PDAs, tablets, etc., and the Internet for legitimate Northern Virginia Cigarette Tax Board ("NVCTB" or the "Board") business, in order to protect the Board and its employees from risks including virus attacks, a compromise of network systems and services, and legal issues associated with inappropriate use of technology.

II. POLICY

NVCTB relies heavily upon internal and external electronic hardware and software information systems used to efficiently store, retrieve and process information. The security, reliability, and integrity of the technological resources and information networks are of vital importance to the continued successful operation of NVCTB.

In addition, NVCTB provides access to the Internet for legitimate Board business and job-related pursuits, such as research, communication, and to provide assistance for wholesalers, vendors, retailers and others interested in the rule and regulations surrounding the possession, transportation, and sale of cigarettes within the jurisdiction of the Board. General usage may consist of research that assists in performance of job responsibilities, research that assists in job-related professional development, sending and receiving email, and researching and purchasing items for use in Board business. Purchasing of supplies and materials over the Internet will comply with regular Procurement policies.

All electronic devices, including desktops, laptops, telephones, cell phones, PDAs, tablets, etc. are provided to employees for the purpose of conducting Board business in the most effective and efficient manner.

The Board provides access to information systems to authorized users for the purpose of conducting official Board business. Each user is responsible for ensuring that his or her use of the Board's information system is legal, ethical, and responsible.

All employees are required to comply with this policy. Failure to adhere to this policy may result in disciplinary action, including termination of employment.

III. SYSTEM ADMINISTRATION

The Information Technology employees shall have administrative responsibility for all Board Computer hardware, software, electronic devices, and data resources.

IV. USE OF ELECTRONICE DEVICES AND COMPUTERIZED INFORMATION

The NVCTB prohibits the dissemination of Board owned or shared information, in any form, contained in or accessed through the Board's computers, to any other person, except one who is officially entitled to receive such information.

Accessing or attempting to access systems, files or documents belonging to the Board or a third party, when not related to the performance of your job assignment is prohibited. For example, attempting to access or view anything in the Board's information network for the purpose of satisfying curiosity is clearly inappropriate.

Employees learning of or suspecting any misuse of electronic devices, security violations or vulnerabilities to the system should immediately notify the Administrator.

V. PERMITTED USES

The following uses are permitted on the Board's electronic devices:

1. Using the Internet only for legitimate Board purposes related to authorized activities of the NVCTB. Internet usage will be subject to all other Board personnel policies. Employees are responsible for determining that their usage of the Internet complies with all Board policies.
2. Incidental personal use of email, Internet access, or voicemail is permitted with the approval of the Administrator. While incidental personal use is allowed, such personal use must not interfere with employees' job duties. Storage of personal email messages, voice messages, files and documents within the Board's information resources shall be nominal. Storage of such personal data in the cloud is preferable so that it is not kept on Board devices. Files maintained on Board devices may be scanned, read, or deleted at any time if the need arises for system maintenance or at the request of the Administrator. All messages, files, and documents, including any user's personal documents, located in Board information resources may be subject to auditor records requests, Freedom of Information Act (FOIA), or for legal purposes, and may be accessed in accordance with this policy. Use of Board electronic devices for accessing social media, such as Facebook or LinkedIn, is prohibited except when done for Board purposes.

VI. PRIVACY

Employees have no expectation of privacy beyond those accorded non-employees in the files stored on Board electronic devices or storage devices. These files may be accessed by the Administrator without notice. The assignment or use of a system password implies no ownership rights or any expectations of privacy on any Board electronic device.

VII. REMOTE ACCESS POLICY

The purpose is to define standards for connecting to the Board's communication networks from any host. These standards are designed to minimize the potential exposure to the Board from damages which may result from unauthorized use of the Board's resources. Damages include the loss of sensitive or Board confidential data, intellectual property, damage to public image, damage to critical Board internal systems, etc.

This policy applies to all Board employees, contractors, authorized agents with a Board-owned or a personally-owned computer/device used to connect to the Board's communications networks. This policy applies to remote access connections to do work on behalf of the Board, including reading or sending e-mail and viewing Internet, intranet, extranet web resources and all telecommuting situations.

Remote access implications that are covered by this policy include, but are not limited to dial-in modems, frame relay, ISDN, DSL,VPN, SSH, and cable modems, etc.

1. Use of remote access is restricted to authorized Board employees, contractors, and Authorized Agents as designated by the Administrator and is for the sole purpose of conducting Board business.
2. The user shall review any related Board policy/policies for details of protecting information when accessing the Board's communications networks via remote access methods, and acceptable use of the Board's communication networks.
3. All hosts, including personal computers that are connected to the Board's communication networks via remote access technologies must use the most up-to date anti-virus software.
4. Personal equipment that is used to connect to the Board's communication networks must meet the requirements of the Board for remote access.
5. Individuals who wish to implement non-standard Remote Access solutions to the Board's production networks must obtain prior approval from the Administrator.

VIII. PROHIBITED USES

The following uses of electronic devices and the Internet is prohibited:

1. Obtaining information or using any Board resources in violation of any law, regulation, policy, procedure, or other rule.
2. Using any Board resource for access to or distribution of indecent or obscene material or child pornography.
3. Releasing or using records for personal or financial gain, or to benefit or cause injury to a third party.
4. Harassing other users, or tampering with any electronic device, and/or damaging or altering the software or firmware components of same.
5. Using Board resources for fundraising, commercial or political purposes, benevolent association activities, or any other activities not specifically related to a business necessity of the Board.
6. Any activity which adversely affects the availability, confidentiality, or integrity of any system resource and/or related date.
7. Engaging in acts that are deliberately wasteful of computing or network resources or which unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, intentionally placing a program in an endless loop, broadcasting unsolicited mailings or other messages unrelated to the business necessity of the Board, creating unnecessary output or printing, or creating unnecessary network traffic.
8. Failing to abide by third party security agreements governing the authorized access and use of relevant databases.
9. Viewing, selling, or purchasing merchandise for personal gain or operating a business utilizing Board electronic resources.

10. Sending or receiving documents that are obscene, offensive, slanderous, or indecent in nature, or that explicitly or implicitly refer to sexual conduct.
11. Conducting illegal, unethical, or irresponsible activities.
12. Compromising the integrity of the Board or operation in any way.
13. Downloading public domain or shareware for use on Board electronic devices without prior written consent of the Administrator, and without proper virus scanning procedures prior to downloading such shareware onto Board devices.
14. Signing up for any services that will incur a cost to the Board, unless previously approved by the Administrator.
15. Sending or receiving documents that violate copyright laws, or any other laws of the Board, the Commonwealth of Virginia, or the United States.
16. Use of Board electronic devices for personal business, except as provided in Section V. (2) above.
17. Sending or viewing any material that contains racial, sexual, ethnic or other content that may be perceived as abusive, harassing or insulting.
18. Sending any message that is intimidating, harassing or threatening.
19. Deliberate activity that damages or impairs system operations, including but not limited to, utilizing streaming video or audio not directly related to the performance of assigned duties.
20. Deliberate display or transmission of information or software that contains a virus.
21. Unauthorized disclosure of the Board's confidential or proprietary information.
22. Visiting game playing sites or playing games.
23. Loading software programs on Board devices, except as authorized by the Information Technology department or the Administrator.
24. Use for personal profit generating activities or excessive personal use including, but not limited to, outside employment, online sales or job searches.
25. Using information resources and electronic devices for public relations or political activities not specifically related to Board activities.
26. Sharing Board accounts, passwords, personal identification numbers, or similar information or devices used for security identification and authorization purposes.
27. Downloading non-work related programs or applications.
28. Using non-standard shareware or freeware without approval of the Information Technology department or the Administrator.
29. Using peer-to-peer or other information sharing software unless approved by the Information Technology department or the Administrator.
30. Attempting to access any data or programs contained on Board systems without authorization or explicit consent.
31. Creating, maintaining, or participating in non-work related Web logs (blogs) or Wikis using Board devices.
32. Creating, maintaining, or participating in non-work related podcasts using Board electronic devices without explicit authorization by the Information Technology department or the Administrator.
33. Degrading the performance of information resources.
34. Depriving an authorized Board user access to a Board resource.
35. Obtaining extra resources beyond those allocated.
36. Circumventing Board information security measures.
37. Downloading, installing, or running security programs or utilities that reveal or exploit weaknesses in the security of a system.
38. Allowing any non-authorized user to access Board systems.

39. Deleting, erasing, altering, or formatting Board storage devices, directories, files, or folders created by the Administrator or user without authority to do so.
40. Copying or otherwise creating an image of any program without authorization of the Administrator.
41. Copying or otherwise creating an image of any file not specific to the performance of job requirements without authorization of the Administrator.
42. Configuring, modifying, partitioning, or altering any predefined hardware, software, or firmware configuration setting located in any Board electronic device.
43. Equipping or attaching an external communication device designed for remote operation or connection without prior written authorization from the Administrator.
44. Operating a Board system resource or Board electronic device while utilizing a password or access privilege other than an employee's own.
45. Using Board electronic devices in a way that is not related to Board business or that is deemed, in the sole discretion of the Administrator, to be inappropriate and inconsistent with board policies.

The above list of prohibitions is not all inclusive. All Board employees must be aware at all times of the importance of the proper, safe and legal, legitimate use of the Internet and technology generally and will be held accountable for not adhering to the highest standards.

IX. SOFTWARE

It is the policy of the Board to comply with all state and federal regulations governing the use of computer software. Illegal or unauthorized use of software may have severe consequences, including legal action for an injunction barring further use of the software and actions for monetary damages and penalties.
In most cases, but not all, the Board does not own all rights to software developed by a third party. Instead, the Board's rights are governed exclusively by a license agreement. Unless expressly authorized by the license agreement, the Board does not have the right to reproduce either the software or its related documentation. It is the policy of the Board to respect all computer software copyrights and to adhere to the terms of all software licenses to which the Board and its employees are a party.

The Board prohibits the illegal duplication or use of computer software, whether developed by its own employees or by third parties.

Each employee using original issue, commercial copyrighted software shall do so only in accordance with any applicable license agreement. Board proprietary software is to be used only to conduct Board business and is not to be copied for personal use or transferred to third parties for use without authorization and without execution of appropriate licensing documentation. Upon termination of employment, the employees shall return to the Administrator all Board owned and third party software in their possession.

Employees learning of such misuse of software or related documentation or who have questions pertaining to said same should contact the Administrator.

X. PURCHASING/MODIFIYING/INSTALLING COMPUTER SOFTWARE OR HARDWARE

Since programs installed on a local device may interact negatively with existing programs, only programs authorized by the Administrator will be installed, loaded, or otherwise used on a Board electronic device.

XII. USE AND CARE OF EQUIPMENT

Employees are reminded that the Board's electronic devices are of vital importance to the productivity of the Board. These costly and environmentally sensitive electrical devices require proper use and care. Do not damage hardware, electronic systems, networks, or devices.

Violations of this policy will result in disciplinary action up to and including immediate termination.

I have read and understand the Internet and Technology Usage Regulations as enumerated above and agree to adhere to said policy.

_____ _____

Signed Dated

_____

Printed Name