County of Nassau, State of New York
Traffic Management Center
Westbury, New York

Internet Usage Policy

Prepared by: P. B. Banaszek

Revised: July 2017

1 Internet Usage as a Privilege

It should be known by all employees of the Nassau County Traffic Management Center that access to the internet for personal use at the workplace is a privilege and not a right. Those who do not comply with the terms of the Internet Usage Policy will have their access to the internet revoked until it has been determined they have a firm understanding of the Internet Usage Policy. Those who choose not to abide by the rules and regulations of the Internet Usage Policy will have their access revoked permanently. This is not to be viewed as a punishment but rather as a safeguard.

2 Trusted Wireless Devices

Each wireless device must be authorized by the Traffic Management Network Engineer. The TMC access point has been configured in such a way that the SSID (The displayed Wi-Fi name) will not be visible until the MAC address of the device is added to the Trusted Devices list. This is considered as a form of Access Control to deter unwanted connections and rogue devices that may attempt to infiltrate the network. Once a device has been approved it will be added to the list of Trusted Wireless Stations which will allow for connectivity to the internet VLAN. Keep in mind all wireless network traffic is being monitored with both passive and active forms of network monitoring software and devices.

3 Email Usage

Email has become an integral part of communication for any organization and the Traffic Management Center is no exception. Employees of the Traffic Management Center are required to access email for their day to day tasks and are also allowed to access their personal Email accounts during their downtime, which includes accessing emails via the Outlook application or the web browser. We advise all employees to remain aware of their login status on any form of email client. In other words be sure to log out of your email account before leaving a workstation unattended. Leaving your email account open compromises your confidentiality and the overall integrity of our network.

3.1 Email Security

The only email issues we typically encounter involve employees who are unaware of potential email exploits; this includes phishing, social engineering, malware, etc. We ask that employees are mindful when clicking hyperlinks or opening attachments, especially if the sender is not someone they know. Users should also pay attention to detail, such as minor grammatical errors or someone asking for username/password credentials. The helpdesk will never ask you for your username or password. These should be seen as red flags indicating an attempt to do harm. It is also important to pay attention to the senders email domain. In most cases, by the time an intrusion is detected it is already too late to reverse the damage. Employees should stay vigilant and report any suspicious emails to the IT department.

4 Internet Browsing

Employees who wish to use the internet for personal internet browsing must only do so on approved devices. Wireless devices must be preapproved as mentioned above and only certain workstations will be delegated for personal Internet Browsing. Currently NCWST9 is the only workstation approved for personal internet browsing due to the fact that it is the only workstation in the demilitarized zone (DMZ). Using any other workstation not only jeopardizes the integrity of the network but also creates more broadcast traffic on that particular VLAN. All offenses will be reported to management.

4.1 Web Filtering

Web Filtering via OpenDNS has been implemented to prevent users from accidently accessing websites that have been compromised or could do harm to the local network. Only approved sites are allowed though the network and any attempt to bypass this safeguard will result in disciplinary action. Employees are not permitted to access content from questionable websites such as gambling, nudity, dating, etc. If an employee wishes to have a website unblocked they may submit a petition to have the website reviewed by the Network Engineer. If the website is deemed acceptable, the website will be added to the DNS whitelist, otherwise the website will be kept on the blacklist. Any attempts to go around the OpenDNS server or to use a VPN connection to bypass these safeguards is taken as a serious offense and will be reported to management.

4.2 Web Monitoring

All network traffic is monitored as part of the Network Security Policy. Any unapproved activity will be reported directly to management. This includes, but is not limited to, web browsing on unapproved devices, using the internet for leisure during peak work hours, connecting unapproved devices such as workstations from home or personal routers to the physical network, etc. As mentioned before, personal internet browsing must be done on approved devices only. The intention is not to make things more difficult for the user, but rather provide a safe work/browsing environment.

5 Application Downloads

Employees must get approval before downloading and installing any form of software or updates. No instant messaging software or applications, such as dating or other forms of instant messaging are permitted. Improper handling of a software installation could compromise the host machine or create compatibility issues with currently running software. Illegal downloads such as torrents or unlicensed software are highly forbidden. Any attempts to do so on the local network will be reported to management and/or the authorities. Those who agree to the terms of the Traffic Management Internet Usage Policy will be made aware of what is considered a legal download and will be held accountable for all of their actions outside of the local network.

6 Personal Internet Usage

All operators should be aware of the restrictions of internet usage at peak times. This includes, but is not limited to, using social media (*with the exception of posting traffic incidents*), shopping, using applications that require internet access (u*nless work related*), VoIP, services that require a large amount of bandwidth, chatrooms, video chat applications, etc. Monitoring has been put in place to track the amount of bandwidth a device uses at peak times. Should a device go over the typical threshold, management may ask for the incident to be further investigated. This is not to say operators are forbidden from using the internet at peak times but rather to use it in moderation and focus on their work responsibilities. It should also be known that these activities are not prohibited during non-peak times and in some cases these actions are encouraged.

6.1 Peak Times

Peak times will be set at the discretion of management and known by all operators before any consequences will be enforced. Aside from peak times operators should be aware of ongoing incidents and daily responsibilities. If having internet access becomes too much of a distraction for an operator, the privilege will be revoked.

7 Further Inquires

For any questions or concerns about the network or the way in which devices are monitored and safeguarded please reach out to the Traffic Management Network Engineer.

Email: Pbanaszek@nassaucountyny.gov

For any further questions regarding peak times, operator responsibilities, or management concerns please refer to the Operator Supervisor.

Email: amoore@wileyengineering.com

8 Acknowledgement and Agreement

This is to acknowledge that I have received, read, and understood the Nassau County Traffic Management Center Internet Usage Policy, and understand that it sets forth the terms and conditions of personal internet usage at the Nassau County Traffic Management Center. I understand and agree that it is my responsibility to abide by the rules, regulations, and standards set forth in the Internet Usage Policy.

I also acknowledge that the foregoing agreement concerning my personal internet usage at the Nassau County Traffic Management Center may be, at any time, altered, changed, or revised in any way during my duration of employment at the Nassau County Traffic Management Center.

_____

Date

_____

Employee Signature

_____

Employee Name [Printed]