INFORMATION TECHNOLOGY

Division:	ADMINISTRATION
Chapter:	INFORMATION TECHNOLOGY
Policy:	INTERNET ACCEPTABLE USE
Section:	PURPOSE, SCOPE, POLICY
Issue Date:	OCTOBER 23,2012
Revised:	MAY 11, 2017

I. PURPOSE

Access to the Internet through the Department of Public Safety (DPS) network and computer systems opens a wide array of new resources and new services for its employees. However, these new opportunities also bring new risks. The Department controls Internet access to safeguard against a multitude of threats and grants access only to those employees who have a legitimate need for it. The ability to surf the web and engage in other Internet activities is not a fringe benefit to which all employees are entitled.

II. SCOPE

This policy applies to all employees, including permanent, contractual, and consultant employees who work for the Department of Public Safety and use the Department of Public Safety computing and networking resources. All users are expected to become familiar and comply with the guidance provided herein. Questions regarding this policy should be directed to the Department of Public Safety's Information Security Office (Statutory and/or Regulatory Authority: Statewide Information Security Manual; § 143B-1376).

III. POLICY

1. Personal Use. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of the Internet. Moderate personal use of the Internet will be tolerated but ***excessive personal use is prohibited*.** Department of Public Safety policy does not allow for unrestricted personal use of the Internet. Users must adhere to other Department of Public Safety and State acceptable use polices which prohibits employees from visiting certain web sites at any time.

2. Prohibited Activities. With the exception of an authorized task or assignment, Department of Public Safety employees are ***strictly prohibited*** from visiting certain types of websites. The items listed below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use:

a. Pornography Sites. Any site containing either graphic or text depicting, describing or otherwise endorsing explicit sexual acts, sex crimes, deviant sexual behavior, rape, sexual products or services, sexually provocative attire and gratuitous or full/partial nudity.

b. Adult Sites. Any site containing profane and vulgar language, expletives, revealing attire, nudity, adult situations, or criminal activity.

c. Violence Sites. Any site portraying or promoting injury, death or torture of human beings or animals, cult or ritual violence, suicide, malicious property destruction, and any site providing instructions on how to carry out these acts.

d. Hate Sites. Any site that contains defamatory speech or activity directed towards a particular group based on race, ethnicity, religion, gender, sexual orientation or social status including sites operated by militant groups.

e. Illegal Activity Sites- Under no circumstances is any employee, contractor or consultant authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Department of Public Safety owned resources

3. Information Reliability. There is no quality control process on the Internet. There is a considerable amount of information that is outdated, inaccurate, and in some instances deliberately misleading. Information taken from the Internet should always be considered suspect until confirmed by another information source.

4. Internet Streaming[1]. Streaming sites (e.g. You Tube, Pandora) consume a large amount of computer network bandwidth which degrades performance.

[1] Internet Streaming is defined as those Internet sites providing information or data in a continuous stream, such as but not limited to video, audio and tickers (news, radio, weather, stock quotes, sports, etc).

Therefore, visiting sites that stream data is only allowed if such use supports an authorized business function. Personal use of these sites is prohibited.

5. Internet Web Page. All Department of Public Safety Internet web pages must conform to layout, navigation, and legal wording standards as well as handicapped accessibility and other applicable requirements specified by the department. Unofficial World Wide Web pages dealing with Department of Public Safety products or services are prohibited unless specifically authorized by the MIS/IT and department management.

6. Unauthorized Downloaded Software. Bringing software from home or downloading unauthorized software and installing it on a Department of Public Safety personal computer or network is strictly prohibited. However, if a legitimate business need exists for a particular file or piece of software, it must be approved and installed by appropriate IT personnel.

    a. Desktop streaming programs (e.g. Weather Bug) shall not be installed on any Department of Public Safety system. Desktop streaming applications consume valuable system resources.

    b. Instant messaging programs shall not be installed on any Department of Public Safety system.

    c. Games shall not be downloaded or installed on any Department of Public Safety system.

    d. Web mail attachments from third party email systems (e.g. Hotmail, Yahoo Mail, etc.) shall not be downloaded to any Department of Public Safety system unless there is a specific business requirement.

    e. Peer-to-Peer (P2P) software (e.g. Frostwire, Limewire, Kazaa, etc.) shall not be installed on any Department of Public Safety system.

7. Unauthorized Uploaded Software. No software shall be uploaded which has been licensed from a third party, or which has been developed by the

Department to any other computer via the Internet. If a legitimate business need exists, it must be approved by the department.

8. Blogging. Blogging by employees (e.g. Twitter) is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of department systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate department policy, is not detrimental to the department's best interests, and does not interfere with an employee's regular work duties. Employees may also not attribute personal statements, opinions or beliefs to the department when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the department. Employees assume any and all risk associated with blogging. Blogging from department systems is also subject to monitoring.

9. Internet Privacy. Internet communications are not automatically protected from viewing by third parties. Unless encryption is used employees should evaluate whether they should send confidential or sensitive information over the Internet.

10. External Access. With supervisory authorization and appropriate authentication, Department of Public Safety employees wishing to establish a connection with the Department's network from an outside source such as an Internet Service Provider (ISP) via the Internet is acceptable.

11. Reporting Problems. Immediate reporting of Internet security violations or problems to the Information Security Office is essential in order to affect prompt remedial action. Immediate reporting is necessary to limit losses from system penetrations and other potentially serious security problems. Delays in reporting can mean massive additional losses for the Department.

    a. Should sensitive material or data become lost, stolen, or disclosed to unauthorized parties, or is suspected of being lost, stolen, or disclosed to unauthorized parties, the user must contact the Information Security

Office immediately. This information must also be communicated to the Chain-of-Command.

b. If passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen, or disclosed, the password must be immediately changed. The Information Security Office shall also be immediately contacted.

c. Unusual system behavior, such as missing files, frequent system crashes, misrouted messages or other indications that the system has a computer virus infection shall be reported to the appropriate Helpdesk or the Information Security Office immediately.

12. Violations. Violations of this policy may result in revocation of privileges, restricted access to network systems, and/or other appropriate disciplinary action, up to and including dismissal. The Department of Public Safety reserves the right to monitor all network assets, including employee Internet usage.