CITY OF PHILADELPHIA

Issued: Effective: Revised: Revision #: 1.0	**Information Security Policy** **Internet Use and Access**	Policy Number: 10.00 Approved By:

1 PURPOSE

This *policy* establishes *general standards* for use of and access to the *Internet.* The purpose of this *policy* is to enhance the ability of City *information users* to perform their job responsibilities and to conduct City of Philadelphia (City) business by providing them with appropriate access to *information* available from the *Internet,* and the capability of appropriately sharing *information* over the *Internet,* among City *information users*, and with Philadelphia citizens and others.

2 POLICY SCOPE

This *policy* applies to all forms of use of and access to the *Internet* by City *information users*. It applies to all such use and access by means of City *information systems* and/or City *networks*, whether by means of City or non-City *messaging* or *Internet* access accounts, by wireless or wireline devices (including by modem over a City or other telephone line), through a City or non-City *Internet Service Provider* (*ISP*) or online service, or by other means, including but not limited to, mainframe computers, servers, personal computers, notebook or laptop computers, hand-held and other mobile devices, *personal digital assistants* (*PDAs*), pagers, *messaging systems* and *network* attached and computer controlled medical and laboratory equipment.

3 USERS

The *users* to which this *policy* applies are all City *information users* that use and access the *Internet* through means furnished by the City as described in Section 2 above. *Information users* or *users* means and includes City *employees*; *information technology administrators*; officers and elected officials; City divisions, *agencies*, departments, boards and commissions; *City-related agencies*; City *contractors*; and *third party users* that use and access the *Internet* on or from City *information systems*.

4 DEFINITIONS

Italicized terms defined in this *policy* shall have the meanings in this *policy* that are here defined. Italicized terms not defined in this *policy* shall have the meanings contained in City Information Security Policy No. 13.00: *Glossary of Information Security Terms.*

5 POLICY

All means of *Internet* access furnished by the City on or from City *information systems* is exclusively the property of the City. All *information* that is created, received, transmitted, stored, deleted and/or otherwise processed using such City furnished means of *Internet* access, including but not limited to, *messages* and *information* that is downloaded from or uploaded to *Internet* sites, is the property of the City or, to the extent provided by applicable law, of the non-City person or entity that created or owns the copyright to the *information*. All such *information* is intended to be used to conduct the official business of the City. City *information users* have no right to privacy with respect to any such *information,* and should not expect nor assume privacy or *confidentiality* with respect to any such *information*. All such *information systems* and *information* are subject to access, *monitoring*, inspection, investigation, disclosure to an investigative authority, and retention by the City at any time without advance notice to the *user*, all in accordance with City *policy* and applicable federal, state and City laws and regulations.

5.1 Standards for Compliance

5.1.1 Acceptable Use

Acceptable use of City-furnished *Internet* access depends upon the specific business needs of the *information user*, as determined by the *user's* job duties and the head of the *user's agency*. *Internet* access is a limited resource provided by the City for use in carrying out job responsibilities and to support the *user's* ability to conduct City business.

Limited occasional use of the *Interne*t furnished by the City on or from City *information systems* for personal communications is permissible to the extent authorized by the head of the *user's agency*, but is strictly subject to the *agency's policies* governing such personal use, and to all other applicable *information security policies* and personnel *policies* of the City. City *information users* have no right to privacy with respect to any such personal communications, and should not expect nor assume privacy or *confidentiality* with respect to any such communications. Personal use is never permissible, however, if it disrupts or compromises the *security* of City *information* or the operation of City *information systems*.

5.1.2 Unacceptable Use

The City considers the following activities to be unacceptable. *Users* are strictly prohibited from knowingly or intentionally engaging in any of them. This list is not exhaustive. *Users* should contact the *Information Security Group (ISG)* if they have questions about the permissibility of a specific use of City-furnished *Internet* access on or from City *information systems.*

a) Sharing *Internet* accounts, passwords, and other types of authorization assigned to individual *information users*. All *information users* are assigned a unique username and password for *Interne*t access. An *information user's Internet* account is for the sole use of the individual to whom it is assigned and this account "owner" is responsible for any inappropriate use of the account, including use by others. Usernames and passwords should never be shared.

b) Using the *Interne*t to download or transfer *software* to others without the approval of the *Information Security Group. Software* downloaded to City *information systems* from the *Internet* may contain *computer viruses* or otherwise interfere with the operation of City *information systems* or *networks. Software* is licensed to the City for the City's use only and may not be made available for use by anyone who is not a City *information user.*

c) Establishing an *Internet* site or an account or profile on an existing *Internet* site or networking site (such as, but not limited to, Facebook, MySpace, LinkedIn, Blogger, YouTube, or Twitter) in the name of the City or any City *agency*, or on behalf of the City or any City *agency*, without the approval of Chief Technology Officer or their designee; *posting* communications or *information* on the *Internet* or any non-City *network* or telecommunications system in the name of the City or any City *agency*, or on behalf of the City or any City *agency*, without approval of the Chief Technology Officer or their designee.

d) Using City *information systems* or City-furnished *Internet* access to create, host, or maintain personal *Internet* sites or pages.

e) Using City *information systems* or City-furnished *Internet* access to communicate or transfer *information*, or to send *messages* that:

   i) Infringe the copyright, trademark, or other *intellectual property rights* of third parties including, but not limited to, creating or transmitting *messages* that contain copyrighted materials without the permission of the copyright owner;

   ii) Violate law or City *policies*;

   iii) Contain language that is defamatory, fraudulent, harassing, offensive, hostile, illegal, or discriminatory;

   iv) Display sexually explicit images, cartoons, jokes, *messages*, or other material in violation of the City Policy Preventing Sexual Harassment in City Government; and

   v) Violate Section 10-107 of the Philadelphia Home Rule Charter, relating to “Political Activities.”

f) Posting or otherwise distributing *for official use only* or *confidential information* on or by means of the *Internet* (including but not limited to, *posting* on *bulletin board services*, *blogs* or other *Internet* sites) and distribution by *listserv* or any other form of *messaging* to unauthorized persons or entities in violation of the City’s Information Security *Policies* No. 10.0: *Electronic Mail and Messaging* or 07.00: *Acceptable Use.*

5.1.3 Monitoring and Disclosure

Consistent with the *policy* stated above, the City reserves the right, subject to applicable law and City *policy*, to *monitor*, access, inspect, copy, retain, and investigate, all *messages* and other *information* created, received, transmitted, stored, deleted and/or otherwise processed using City-furnished means of *Internet* access; and to disclose any such *messages* and *information* to law enforcement agencies and other investigative authorities for the purpose of carrying out their official duties. Such *messages* and *information* may also be subject to disclosure in litigation and under the Pennsylvania’s Right to Know Act, 65 P.S. §§ 67.101 et seq. and or Section 5-1104, “Public Inspection of Records,” of the Philadelphia Home Rule Charter.

a) The *ISG* and its designees have the exclusive right to monitor and inspect an individual *user’s messages*, and will do so in the normal course of business to ensure the *security* of City *information systems* and/or at the request of a City investigative authority or a law enforcement *agency*.

b) In order to ensure the *security* of City *information systems*, the City's *Internet* access system filters requests and controls the content of *web* pages based on rules established by the City and implemented by the *ISG*.

c) In order to ensure the *security* of City *networks*, the City *monitors* and maintains electronic records of *Internet* access and use by means of City *information systems* connected to City *networks*. For all *Internet* traffic, the City logs the *Internet* sites and addresses accessed by each *information user*, the *network* address of the computer from which access is obtained, the number of times each site is accessed, and the time spent at each site. *Internet* use is logged to enable investigations, system capacity planning, and reports to appropriate City officers, including *agency heads* (for *Internet* use by *agency employees*), the City's Chief Technology Officer, the *ISG,* and for other reasons deemed appropriate by the City. Upon request by an authorized City officer, the *ISG* will generate the following *Internet* activity reports:

   i) Aggregate Reports. Aggregate reporting shows trends for multiple *information users* at one time. These reports are used to determine the behavior of a group, such as an *agency*, or sub group. Aggregate reports are available for each *agency* and the sub groups created within that *agency* in the system. These groups are specified by the *agency*. Aggregate reports are made available by the *ISG* with *agency* management (or designees) approval as requested.

   ii) Individual Reports. Individual reporting shows the *Internet* use patterns of an individual *information user*. These reports typically are used during investigations of inappropriate *Internet* use and will not be made available by *ISG* without proper request from or authorization by the *user's agency head* (appointing authority) or designee, the Inspector General, Police Department, Internal Affairs Division, the Law Department, the Ethics Board, and/or the District Attorney's Office. *ISG* approval is required for all disclosures of individual reports.

d) Authorized individuals who maintain and administer City *networks* and authorized managers may, subject to *ISG* approval, *monitor*, review, access, or disclose, and report the contents of *Internet* use logs to authorized City personnel, in the course of carrying out their authorized duties, without prior notice to the *information users* whose activity is logged. Reasons for such actions may include, but are not limited to, assuring proper use of *information*, *messages*, and *information systems*; preventing *security* violations, investigating and controlling excessive and/or inappropriate *Internet* use, or any other reason deemed appropriate by the City. Excessive and/or inappropriate *Internet* use on the part of individual *users* may be investigated, and if in violation of this or any other City *information security policy,* may lead to the removal or restriction of *Internet* access and/or disciplinary action.

e) All *information users* and *information technology administrators* are required to report to the *ISG* any unauthorized or inappropriate use of City-furnished means of *Internet* access they discover or suspect, and any breach of *information security policies.*

5.1.4 Internet Connectivity

Information systems connected directly to the *Internet* create a serious and unacceptable risk to City *information systems* and *information. Agencies* and *information users* are strictly prohibited from connecting any *information system* to the *Internet* directly, i.e., by any means that does not connect through *firewall(s)* and *proxy servers* managed by the Division of Technology (e.g., connection by

modem and telephone line, wireless connections from a personal computer connected to a City *network* to a Wi-Fi "hotspot.") Any *user* who is uncertain whether an *Internet* connection is prohibited should contact the *ISG*. The Division of Technology (DOT) has sole responsibility and authority to manage and control means of connecting to and accessing the *Internet* from City *information systems*.

5.1.5 Administration of Internet Access

The City's goal is to provide *Internet* access to all *information users*, but *Internet* access accounts are subject to availability, as determined by the capacity of the *networks* and equipment used for *Internet* access.

5.1.6 Exception Management

This *policy* is not intended to preclude the use of City *Internet* access to meet any legitimate business need of the *user* or the *user's agency*. If an *agency* needs to transmit or access materials prohibited by this *policy* or otherwise to act contrary to the *policy* in order to conduct its business and carry out its responsibilities, the *agency* is responsible for first obtaining approval for an exception to the *policy* from the *ISG.*

6 ENFORCEMENT: DISCIPLINARY ACTION

Each City *agency head* shall be responsible for enforcing compliance with this *policy* by *agency information users.*

Information users that violate this *policy* may be subject to disciplinary action, up to and including, termination of employment, in accordance with the disciplinary *policies* of the *information user's agency* and, for *information users* represented by the Fraternal Order of Police, International Association of Fire Fighters, District Council 47 or District Council 33, the terms of the applicable collective bargaining agreement.

If a City *contractor* or *third party user* knowingly or negligently commits or permits a violation of this *policy*, the City may terminate the contract or agreement in accordance with its terms, and/or terminate the *contractor's or third party user's* access to City *information systems* and *information,* in addition to any legal or remedial actions the City may take to enforce and protect its interests.

7 GETTING MORE INFORMATION

Questions about this *policy* and other *information security* matters should be addressed to the *Information Security Group* ISG@phila.gov).