



# Administrative Directive

Title: Information and Communications Technology Acceptable Use		Index Number: AD 2.04
Date of Adoption: 07/23/96	Date of Revision: 12/20/99 04/01/10	Page 1 of 4

## 1. Purpose and Need

The City of Virginia Beach is committed to protecting its employees, partners and citizens from illegal or damaging actions by individuals that involve the use of the City's communication and information technology systems. Information and communications technology components include: computer equipment, software, smart phones, PDAs, data, operating systems, storage media, network accounts providing electronic mail, Internet browsing, and file transfers. City owned information and communications technology components are to be used for business purposes in serving the interests of the City and of our citizens in the course of normal operations. The City of Virginia Beach's intention for publishing an Information and Communications Technology Acceptable Use Administrative Directive is to foster the City's established culture of openness, trust and integrity by clarifying expectations for employees' use of electronic computing and communications resources.

Effective security is a team effort involving the participation and support of every employee who deals with communications and information systems. It is the responsibility of every computer user to know these guidelines, and to conduct his or her activities accordingly. Acceptable use is based on a reasonable level of common sense, common decency, effective stewardship, and civility as applied to the information and communications environment. The Acceptable Use Administrative Directive is also derived from the City's Code of Ethics, which establishes principles that guide staff conduct in relations with citizens, customers, vendors and contractors, the community and other members.

This directive has been formulated with the following goals in mind:

- To ensure the security, confidentiality, reliability and privacy of the City's information and communications technology systems and the information and communications technology systems of others;
- To avoid situations that may cause the City, its officers and/or its employees to incur adverse publicity, or civil and/or criminal liability;
- To encourage the responsible use of information and communications technology systems and discourage practices that degrade the usability of information and communications technology systems; and
- To preserve the privacy and security of individual Users engaged in the appropriate use of information and communications technology systems by prohibiting improper actions by other Users.

The information and communication technology systems resources and bandwidth are of limited supply. Personal use of the Internet can tax these finite resources particularly when Users utilize high bandwidth sites including, but not limited to: Internet radio, Internet TV, and social networking sites. The effective performance of information and communications technology systems, whether they are local or global, relies upon Users adhering to established standards of proper conduct. Also, as is true with any public resource, individuals who are entrusted with the

Title: Information and Communications Technology Acceptable Use		Index Number: AD 2.04
Date of Adoption: 07/23/96	Date of Revision: 12/20/99 04/01/10	Page 2 of 4

privilege of using the resources of the City's information and communications technology systems must be accountable. This directive defines the responsibilities of officers and employees of the City and of any other individuals who are using information and communications technology systems. In general, the directive requires the appropriate, efficient, ethical, and legal utilization of information and communications technology systems.

## 2. Administrative Directive

A. General Conduct: The City's information and communications technology systems may be used for lawful purposes only. Users shall abide by all applicable contract provisions as well as federal, state, and local statutes, ordinances, rules, and regulations, including, but not limited to, provisions relating to copyright protection. Users shall also abide by the City's policies, administrative directives, procedures, rules, regulations and guidelines, as well as those of the various departments and agencies. Users shall abide by generally accepted information and communications technology systems etiquette. Users shall abide by the AUP of any network that is accessed via the City's network.

### B. General Prohibitions:

1. Users are prohibited from transmitting, distributing, creating, or storing any material if doing so would violate any federal, state, or local common law, statute, ordinance, rule, or regulation. This includes, but is not limited to, any action that would violate copyright, trademark, or trade secret laws.
2. Users are prohibited from transmitting any inappropriate material on or through any of the City's information and communications technology systems. The City has the sole discretion to determine whether material is inappropriate. The City also reserves the right to remove any inappropriate material from its software/hardware. Inappropriate material includes, material that: (a) is unlawful or illegal; (b) is pornographic or obscene; (c) is threatening; (d) is abusive; (e) is libelous; (f) is offensive; (g) encourages or incites conduct that would constitute a criminal offense; or (h) could potentially lead to civil and/or criminal liability or adverse publicity for the City, its officers and/or employees.
3. The intentional use of information and communications technology systems to access, create, transmit, or process obscene or pornographic material, inappropriate text or graphic files, or files that pose a danger to the integrity of the City's information and communications technology systems is prohibited.
4. Users are prohibited from using City email systems to send unsolicited email messages, including the sending of junk mail, chain mail, or other advertising material to individuals who did not specifically request such material (email spam).
5. The use of City-provided information and communications technology systems for an individual's commercial use or profit, or for secondary employment not associated with the City, is prohibited.

### C. Network Security:

1. Users shall not attempt to circumvent User authentication or security of any host, network, or account (sometimes referred to as "cracking"). This includes accessing data not intended for the User, logging into a server or account the User is not expressly authorized to access, capturing network traffic that the User is not authorized to view, or probing the security of the City's network or other networks.
2. Users shall not attempt to interfere with service to any User, host, or network. This includes "flooding" the network, deliberate attempts to overload a service, and/or attempts to "crash" a host.
3. Users shall not disable application security features (audit logs, required passwords,

Title: Information and Communications Technology Acceptable Use		Index Number: AD 2.04
Date of Adoption: 07/23/96	Date of Revision: 12/20/99 04/01/10	Page 3 of 4

access levels, etc.) or virus scanning/checking software, except when authorized by the Information Security and Privacy Office of ComIT.

4. Users shall not use any kind of program/script/command, or send messages of any kind, designed to interfere with another User's terminal session, via any means, locally or by the Internet. Users who violate network security may incur criminal and/or civil liability.
- D. City information and communication systems exist for the conduct of City business. Limited personal use is nonetheless permissible only if the use does not interfere with worker productivity, does not preempt any business activity, does not affect Network security, does not utilize excessive bandwidth, cannot result in legal liability on behalf of the City, and does not result in performance issues by or between workers.
- E. The information and communications technology systems and the information contained therein, as well as individual workstations are the property of the City. The City reserves the right to access any User's workstation and the information stored therein at any time and at the City's discretion. Users should not consider any of the material transmitted via or stored in City information or communications technology systems to be private.
- F. Users have no expectation of privacy during use of information and communications technology systems. For example, electronic communications from an employee's City email account can be considered official business documents. All users should exercise extreme caution when including confidential and personal information in electronic media.
- G. Network accounts are to be accessed only by the Authorized User of the account. The confidentiality of passwords and User accounts shall be protected. Individual Users can be held accountable for the use of their account by others, unless the use occurred through no fault of the User. Users shall not share their passwords.
- H. Users and their department or agency directors are jointly responsible for understanding the provisions of this directive and monitoring the use of information and communications technology systems for Users' assigned duties and responsibilities

3.0 Procedure to Accomplish Administrative Directive

The Communications and Information Technology Department is responsible for communicating the provisions of this directive to all City members.

4.0 Responsibility and Authority

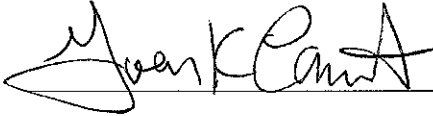
- A. The Information Security and Privacy Office shall periodically review the standards for the acceptable use of the City's information and communications technology systems.
- B. The use of information and communications technology systems shall directly support the assigned duties and responsibilities of the User and the delivery of municipal services. At all times, a User's actions shall be consistent with the specific requirements set forth in this directive to ensure the appropriate, efficient, ethical, and legal use of Information Technology Resources.
- C. In the event of a violation of this directive, the User's agency or department director and supervisor are jointly responsible for determining and implementing necessary action which may include taking action to remove a User's access to information and communications technology systems (including network services and equipment) and, in the case of City employees, for instituting appropriate disciplinary action. Agency or department directors may impose additional requirements that are more stringent than the ones set forth in this directive.


Title: Information and Communications Technology Acceptable Use		Index Number: AD 2.04
Date of Adoption: 07/23/96	Date of Revision: 12/20/99 04/01/10	Page 4 of 4


D. Department directors may request an investigation into a member's use of information and communications technology systems if the director suspects that the member's conduct violates this Directive or if the request is in furtherance of an administrative investigation. The request shall be sent to the Director of Communications and Information Technology.

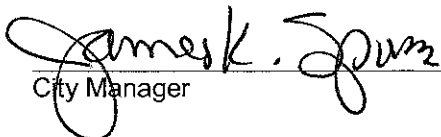
5.0 Definitions

- A. Acceptable Use Policy ("AUP") - A policy promulgated by a network that places restrictions on the use of the information and communication technology. For example, the AUP of the National Science Foundation does not allow the commercial use of its Information Technology.
- B. Authorized User - The individual in whose name the access account has been issued and to whom the password for access was given.
- C. Cracking – Breaking into someone else's computer system, often on a network; bypassing passwords or licenses in computer programs; or in other ways intentionally breaching computer security.
- D. Internet - A global system of interconnected computer networks that use the standard Internet protocol suite to serve billions of users worldwide. It is a *network of networks* that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by a broad array of electronic and optical networking technologies.
- E. Network or Networks - A system of hardware and software interconnected in such a way that data can be transmitted and end Users can communicate.
- F. Information and Communications Technology Systems - Internet, Intranet, e-mail, telephony, radio, and any other services or resources accessed via the City's information and communications technology.
- G. User - Anyone who utilizes the City's information and communications technology systems and services.

Approved as to Content:  \_\_\_\_\_ 4/1/10  
Department of Communications and Information Technology Date

Approved as to Legal Sufficiency:  \_\_\_\_\_ 4/6/10  
City Attorney's Office Date

Approved:  \_\_\_\_\_ 4.16.10  
Deputy City Manager Date

Approved:  \_\_\_\_\_ 4/16/10  
City Manager Date