1403 – USE OF INFORMATION TECHNOLOGY

I. PURPOSE

The purpose of this Policy is to ensure appropriate, responsible, and safe use of information technology, including the internet, in serving the interests of the City of Newport News, its clients and customers, in the course of City operations.

II. APPLICABILITY

This Policy applies to all City employees and to all City technology. No informal practices are to be construed as acceptable deviations from this policy. However, department heads may supplement this policy for specific operational needs, in accordance with the City's Personnel Administrative Manual, Section 101-Personnel Policies and Procedures.

III. RESPONSIBILITY

A. City Employees shall:

1. Receive and review this policy, and sign an acknowledgement form;

2. Comply with all policy provisions.

B. Directors shall:

1. Approve City employee access to City technology;

2. Ensure all City employees read and acknowledge receipt of this policy;

3. Enforce policy compliance;

4. Consult with the Director of Human Resources and the City Attorney's Office prior to any search of City technology, including emails, messages, images, and files contained therein, for suspected employee misconduct or criminal conduct.

C. The Department of Information Technology (DIT) shall:

1. Manage, administer, and provide access to City technology unless an exception is granted by the department. Exceptions may be specific to a particular use, a specific function, or an entire department, in which case it will be specified in writing which group is assuming responsibility;

2. Support policy compliance;

3. Respond to requests for access to City technology and electronic records in any investigation involving suspected employee misconduct, and coordinate with the Department of Human Resources and City Attorney's Office as to activities related to such requests.

IV. DEFINITIONS

A. Backup - Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a disruption.

B. City Technology - All information technology resources, including but not limited to computer networks (including email, Intranet, Internet, etc.), hardware, software, systems, programs, and devices (including cell phones, personal digital assistants, tablets, pagers, storage media, etc.) supplied, owned, or operated by or for the City of Newport News for use in City business. City technology includes all such information technology resources of the City's contractors and Third-Party Service Providers which are provided to City Employees for use in City business.

C. DIT - The Department of Information Technology. The department responsible for Citywide information systems, networking, and data management.

D. Device - Any device that is capable of receiving or transmitting City data to or from City Information systems.

E. Electronic Records - Consist of computer records and files, emails, text messages, voice messages, images, web pages, logs, audio and visual recordings, and optically scanned records, also known as machine-readable records, that are created, viewed, manipulated, stored, retained, sent, or received, by electronic means in, by, or through City technology. Most Electronic Records are also Public Records under the Virginia Freedom of Information Act and the Virginia Public Records Act, and are referred to as Electronic Public Records.

F. Information - Any and all data, regardless of form, that is created, contained in, or processed by, information systems facilities, communications networks or storage media.

G. Information Systems - Any and all computer-related equipment and components involving devices capable of managing, transmitting, receiving or storing information or data including, but not limited to, a USB drive, CD-R, laptop or personal computer, personal digital assistant (PDA), cell phone, handheld computer, servers and computer printouts. Additionally, the procedures, equipment, facilities, software and data that are designed, built, operated and maintained to create, collect, record, process, store, retrieve, display and transmit information.

H. Internet - A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies and educational institutions.

I. Intranet - A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization.

J. Owner - The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

K. Password - A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data. A strong password is one that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, Social Security number, etc.

L. Server - A server is a system that provides services to client systems. The computer that a server program runs in is also frequently referred to as a server (though it may contain a number of servers and client programs).

M. Third-Party Service Providers - Firms that provide services to all or some City employees for use in City business including but not limited to services for the creation, transmission, retrieval, use, or storage of electronic records, including providers of cellular phone service, internet service, message service, and other data and voice transmission services. A Third-Party Service Provider may, but is not required to be, under contract with the City.

N. Trojan - Destructive programs that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a trojan horse program by mail or on a removable media device, often from another unknowing victim, or may be urged to download a file from a Website.

O. User - An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

P. Virus - A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive results. A

file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in programs that allow users to generate macros.

Q. Web Page - A document on the World Wide Web. Every Webpage is identified by a unique URL (Uniform Resource Locator).

R. Website - A location on the World Wide Web (www), accessed by typing its address (Universal Resource Locator, or URL) into a Web browser. A Website always includes a home page and may contain additional documents or pages.

V. GENERAL PRINCIPLES

City of Newport News information systems, resources and devices are provided for performing City business. These systems, resources and devices are explicitly owned by the City of Newport News and the City owns all property rights to any content or other matter created, from, any City information system, resource or device. In addition, any City information stored on a user's non-City issued mobile or fixed device is City property and may be viewed, accessed, retrieved, copied or disseminated by the City at any time.

Access to City technology imposes certain responsibilities, limitations, and obligations upon the user or recipient of that access. This use and access must always be ethical, honest, and in the best interest of the City. City employees must also show proper restraint in the consumption of data, adhere to system security mechanisms, and avoid intimidation, harassment and unwarranted intrusion of others.

Users of City information systems are expected to abide by City and departmental policies and procedures, as well as any other applicable local, state or federal laws and regulations, regardless of whether a particular City information system is located internally or remotely, as in a cloud or similar type of off-site data storage, or whether data is transmitted, stored or received on mobile or fixed devices.

Examples of City information systems and resources include, but are not limited to, the following:

- Desktop PCs and workstations
- Servers and network communications equipment
- Mobile devices such as laptops and tablets
- City-issued cell phones, smartphones, and other voice and data devices
- City-provided desktop telephones, projectors, and teleconferencing equipment
- Accessible enterprise resources such as email, instant messaging, internet, and other productivity software
- Remote access technologies that enable secure communications between City-owned and non-City-issued devices

- Other enterprise technologies acquired and approved for enabling electronic access to City resources and data

VI. USER PRIVACY

No City employee, or individual representing the City's interests or conducting business, who is authorized to access City technology shall have any expectation of privacy in City technology, electronic records, web pages, or web sites that are created; visited; manipulated; stored; receive; transmitted or retrieved in, by, or through any City technology; with the exception that any electronic records and other communications in the course of City business which are protected by the attorney-client privilege or the attorney work-product doctrine created, sent, or received by, or at the behest or under the oversite of, the City Attorney's Office or outside counsel retained by the city, shall remain strictly confidential.

In order to access, retrieve, or copy any City technology or electronic records, City employees shall have no expectation of privacy in a City-supplied vehicle, City office, cubicle, or other City work space, and the furniture contained therein, which may be entered, inspected, and searched for this purpose. However, no personal items such as purses, briefcases, clothing, or bags may be searched.

A. Monitoring, Searching and Retrieval of City Technology

The City may, without notice, audit, monitor, inspect, copy, and retrieve, any City technology and any electronic record, or user activity on City-approved mobile and fixed devices, including but not limited to email, messages, files, inbound and outbound file transfers, web sites visited, including uniform resource locator (URL) of pages retrieved, and the date, time, and user associated with each use. Such activity is for the performance of legitimate City business including but not limited to the following:

1. To monitor and evaluate the efficiency, quality, use, and volume of City services, and City technology, and to evaluate the achievement of service goals;

2. To investigate suspected violations of law or City or departmental policies by City employees or third parties, when deemed necessary or appropriate;

3. To audit or monitor networks that connect to the Internet or other publicly available networks to support identification and termination of unauthorized or improper activity;

4. To comply with a law, court order, or other legitimate governmental purpose

DIT and department directors have the right to monitor any and all aspects of the City's information systems, including any chat group, material downloaded or uploaded, and any email sent or received. This monitoring may occur at any time without notice and without the user's awareness or permission. Internet traffic over City information systems shall be proxied and inspected for malicious code or inappropriate content prior to delivery to the user. Filters shall track user internet activity, and be monitored for violations of this policy, as well as any other applicable laws, regulations, and City policies and procedures.

B. Personal Electronic Records

Storage of user personal information on City information systems is done at the user's risk. Such information may be subject to public disclosure or review by City officials. By using any City information system, the user agrees to surrender any data contained in such information system whether the data is owned by the City or alleged to be owned by anyone other than the City.

VII. CONFIDENTIALITY

Users shall comply with all laws, regulations, and City policies and procedures prohibiting or limiting the disclosure of confidential information, including but not limited to City client personal information (e.g. medical records, financial information, and social security numbers), tax information (e.g. information of any person firm or business with respect to any transactions, real and personal property, income or business of the taxpayer) and City employee personal information (e.g. medical records, financial information, and social security numbers). Confidential information transmitted on City information systems shall be sent only to those recipients who are authorized to receive such confidential information. Users shall take all steps necessary to protect the privacy of confidential information maintained by the City from unauthorized access. These measures include, but are not limited to, enabling password protection on any fixed or mobile system, or otherwise locking and closing computer screens when leaving even for brief period, and logging off or terminating a system session when access is no longer needed or the user is leaving for the day. Users shall follow all Federal, Commonwealth, and City policies and guidelines defining data classification and protection requirements. These requirements include, but are not limited to, the following:

- Information classified as confidential or sensitive shall only be stored on approved storage devices that use encryption;
- Users shall not use non-City information systems or devices to send, forward, receive or store information classified as confidential, sensitive, or for "Internal Use," unless approved by DIT in writing;
- Users shall not use non-City messaging utilities such as Hotmail, Yahoo Mail, AOL Mail, and Google Mail to send, forward, or receive information classified as confidential, sensitive or for "Internal Use;"

- Information classified as sensitive being sent outside of any City information system shall be specifically labeled as such and shall have restricted distribution only to those Recipients who are authorized to receive such sensitive information;
- Information classified as confidential or sensitive transmitted to external networks shall be encrypted in accordance with DIT encryption standards.

VIII. INCIDENTAL PERSONAL USE

Personal use of any City information system is use that is not related to the purpose for which the City has granted the user authorized access. In general, incidental personal use of the City's information systems, such as internet access and email, is permitted unless the agency in which the user works restricts all incidental personal use of information systems. Personal use of information systems is prohibited when it:

- Interferes with the user's productivity or work performance, or with the productivity or work performance of other users;
- Adversely affects the efficient operation of the information system or the City;
- Is illegal, or violates City policy or procedures.

Users must present their personal communications using City information systems in such a way as to make clear that these communications are personal, and not communications from their agency or the City or from the user in his or her capacity as a representative of the City. Storage of personal email messages, voice messages, files, and documents on City information systems shall be kept to a minimum. Any such storage which DIT determines interferes with the efficient operation of the City's information systems is subject to removal by DIT without the notice or consent of the user.

IX. PROHIBITED USE

Certain activities are prohibited when using City information systems, applications, data and resources, whether on City–owned or personally–owned devices, except when DIT and Departmental Directors have determined such activities are necessary for the performance of a user's official duties. These prohibited activities include, but are not limited to, the following:

- Accessing, downloading, transmitting, printing, or storing information with sexually explicit content. DIT will be responsible for approving all software loaded onto City technology unless an exception is granted by the director. Exceptions may be specific to a particular use, a particular device, a specific function, or an entire department;
- Downloading or transmitting fraudulent, malicious, threatening, obscene, intimidating, defamatory, violent, harassing, or discriminatory messages or images. Also, using obscene, profane, discriminatory, demeaning, or degrading language; harassing, intimidating, broadcasting unsolicited messages or email or otherwise annoying other persons;
- Accessing or downloading gambling sites;

- Pursuing personal profit or gain (e.g. personal use, family members, relatives, or friends), or engaging in outside employment or personal business, unauthorized fundraising or political activities including the use of email to circulate advertising or other material for candidates;
- Engaging in any prohibited activity described in City policy, procedure, regulation or guidance related to the use of City information systems;
- Unauthorized downloading, printing, or transmitting of information protected by federal or state copyright laws;
- Misusing or misapplying City information system privileges;
- Using software in violation of City vendor licensing agreements;
- Decoding or attempting to decode passwords or encrypted information, or to otherwise circumvent system access control or other security measures;
- Making or using illegal copies of copyright-protected material including software, storing of such copies on City technology or elsewhere, or transmittal of same through City technology;
- Disconnecting or moving stationary City technology without consent;
- Altering the City provided access configurations without specific written authorization by the Director of Information Technology;
- Using "taglines" in any City technology or electronic public record. Taglines are usually phrases, catch-words, slogans, or quotations, which are sometimes added at the end of an email or other written communication, which become identified or associated with a person, group, service, product, etc. Only City or department approved taglines may be included in City technology and electronic public records. (Note: This prohibition also applies to all non-electronic public records created or sent by City employees in the course of City business.)

X. INFORMATION SYSTEM SECURITY

Users shall respect the confidentiality and integrity of any City information system, be familiar with City information-system security policies and procedures, and report any security weaknesses or breaches in City information systems to DIT. Users shall respect security controls for City information systems and not attempt to or circumvent those controls. Users shall not access or attempt to access any City information system without authorization from DIT or department director. Users shall refrain from activities that intentionally or inadvertently disrupt, impair, or undermine the performance of City information systems. These activities include, but are not limited to, the following:

- Intentionally causing physical or logical damage to a City-owned information system or resource;
- Downloading computer viruses or malware or otherwise introducing malicious code into a City information system;
- Using internet-based proxy servers or anonymizers, or any other tool, device or action that makes internet activity untraceable, to bypass web-filtering security mechanisms established on City information systems;

- Downloading, installing, or running security programs or utilities that reveal weaknesses in the security of a City information system, such as password cracking programs, network reconnaissance and discovery applications, key loggers, packet sniffers, network mapping tools, and port scanners, without prior approval from DIT in writing;
- Consuming excessive bandwidth (e.g. placing a program in an endless loop, printing excessive amounts of paper, sending chain letters and unsolicited mass emails, etc.)

Files and other content installed or downloaded from the Internet, including but not limited to non-standard shareware, free software, peer-to-peer software, games, and information-sharing software, is subject to prior approval from DIT or department director in writing. This approval may be conditioned upon DIT checking the downloaded files or content for viruses, trojans, malware, or other potentially malicious content.

Users shall refrain from divulging to unauthorized persons any details regarding City information systems or architecture, unless authorized by the department director and DIT.

The use of strong passwords to access City information systems and City-approved mobile communications devices is for the protection of the City, and not any user. Users shall prevent the disclosure of their USERID, PASSWORDS, security tokens, or other similar information to unauthorized users. Also, using another person's credentials, files, systems, or data without permission is prohibited. Users are responsible for all activities which transpire under their USERID.

Users shall not use cloud or internet-based hosting services to store or share City data unless specifically approved by DIT in writing.

Users shall take all steps necessary to complete logoff/lock or other termination procedures when finished using any City information system. At a minimum, users should take such steps to logoff/lock terminal from a City information system.

Users of City-approved mobile devices shall ensure that precautions are taken to prevent theft or loss. Unattended City mobile devices shall be physically secured (e.g., locked in an office, desk drawer or filing cabinet; attached to a desk or cabinet by a cable lock system) when unattended. Any user must immediately report to DIT or use departmental procedure any loss or theft of any mobile device containing any information from a City information system.

XI. REMOTE ACCESS

Remote access to City information systems shall only be permissible through DIT provided and supported remote access software applications, protocols, delivery mechanisms, and if necessary, DIT provided and supported anti-virus software. Remote access for employees shall be requested by a department director and approved by DIT after a determination has been made that access is required to perform assigned duties, or the user is defined as "essential" personnel by the City.

XII. USE OF NON-CITY ISSUED DEVICES AND PERIPHERALS

Users shall not connect non-City owned equipment or devices including, but not limited to, USB or other storage or memory devices, iPads or iPods, PDAs, tablets, Android devices, mobile phones or cameras, to the City network infrastructure in any manner without approval of the department director and DIT. All such computer equipment and peripherals that are installed or in use as of the effective date of this policy shall be reported to DIT for review. These devices should not be connected to City systems for purposes of charging power, transferring personal audio, video, or images as non-City owned electronic devices may introduce unnecessary risk to City systems and data.

DIT is not responsible for responding to any hardware or software support issues relating to such equipment and or peripherals unless authorized by department director. Remote access to City information systems using a non-City issued device shall only be permissible through DIT provided and supported remote access software applications, protocols, delivery mechanisms, and if necessary, DIT provided and supported anti-virus software. Users with remote access shall ensure that their non-City issued devices remotely connected to a City information system is only connected to legitimately secure networks, such as a personally-owned home network under complete control of the user, or a validated provider network, and that their fixed device or mobile communications device maintains basic security controls (e.g., password protection) to prevent unauthorized access to all City information systems. The method of storing information on non-City issued devices shall comply with DIT information-system security requirements.

In all cases where non-City issued devices and/or peripherals are used in departmental work spaces, the owner of the equipment shall assume full and sole responsibility for the equipment's legal and safe operation and any liability that may result from usage on City property. Users shall immediately report the loss of any non-City issued devices used to access City information systems to DIT. In the event of a lost or stolen device, the City reserves the right to clear its data from the device by any available technical means. The City shall not be responsible for any non-City issued device, software, or peripheral devices that may be stolen, damaged, or otherwise made inoperable while in departmental work spaces. The user shall assume all risk of loss or damage.

In the event that City technology becomes infected with a virus, and the infection is traced to a non-City issued device, or media, the individual transferring the virus to the City technology may be held responsible for the costs of removing the virus and restoration of the electronic public records.

XIII. USE OF ELECTRONIC MESSAGING

City users are responsible for the content of all text, audio-video or images stored or transmitted over the City's electronic messaging (i.e., email) and other collaboration systems, such as instant messaging. All messages communicated on City email systems shall contain the sender's name. Email or other electronic communications shall not be sent on City email

systems which mask or attempt to mask the identity of the sender. Users shall make reasonable efforts to validate the authenticity of emails received prior to opening any attachments or clicking on links.

The following activities are examples of acceptable uses of City email systems:

- Communicating and exchanging information directly related to the mission, charter, or work tasks of the City;
- Communicating and exchanging information for professional development, to maintain currency of training or education, or to discuss issues related to the City business;
- Applying for or administering grants or contracts for City research or programs;
- Conducting advisory, standards, research, analysis, and professional society activities related to the City business;
- Announcing new laws, procedures, policies, rules, services, programs, information, or activities;
- Incidental personal use; users of City email systems shall not give the impression in their communications to persons receiving such emails that they are representing, giving opinions, or otherwise making statements on behalf of the City or any agency of the City, unless otherwise authorized to do so. Where appropriate, a disclaimer shall be included such as, "The opinions expressed are my own, and not those of City of Newport News," unless it is clear from the context that the email's author or sender is not representing the City.

XIV. USE OF INTERNET AND INTRANET

City of Newport News websites which includes the external facing public websites and content, the City-wide Intranet site for internal City applications and services access and other collaboration tools, are for City business purposes. The City provides general access to the Internet from City networks and devices to include social media. Also, when an employee is issued a City mobile device, access to the Internet from that device is identified as a City device. By accessing the Internet from any City IT resource, City users are identified as connecting from City of Newport News. Content and use of all City Internet and Intranet sites shall comply with City IT security policies and standards, Personnel Administrative Manual policies, and any other applicable City policy to include department specific compliance procedures, standards, or guidelines. This includes use and actions on an external website from City of Newport News networks and devices.

Web filtering technologies are implemented that govern policy and access to the Internet from City of Newport News network(s) and devices to protect the City's technology systems and data from exposures to malicious code, excessive bandwidth uses, and also to block content and internet sites deemed to present in its use significant risk, either inappropriate or illegal. City users shall not try to circumvent the implemented web filters or otherwise

tunnel through authorized sites to gain access to unauthorized sites. Internet sites which are blocked but are later determined to be necessary to conduct business on behalf of City of Newport News can be submitted to the IT Helpdesk for review and consideration.

Users shall not download or paste any application, service or inappropriate data from the Internet to the City Internet or Intranet sites without authorization by DIT. Users shall not use the Internet to purchase, obtain, or offer products or information for City purchases outside of City purchasing policies and procedures, or without prior approval from the Office of Purchasing.

XV. TERMINATION OF ACCESS

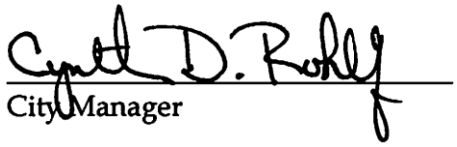
Engaging in prohibited uses of the City's information systems shall be considered a violation of City policy may result in disciplinary action in accordance with City policy. The City reserves the right to deny further access to its information systems when such action is necessary to protect system security and performance. If deemed necessary by the department director, the Director of DIT and the Director of Human Resources, any user's access to City information systems and all City devices shall be terminated, and the user shall return to DIT all City-owned mobile communications devices issued. Access privileges to City information systems through a non-City issued device shall be terminated for any reason deem necessary by DIT to protect the City.

In addition, upon separation from the City, user access to City information systems and all City devices shall be terminated. The user shall return to the department or DIT all City-owned communications devices issued.

Anyone who suspects a user of any inappropriate use of City information systems should direct questions concerning any inappropriate use to their supervisor, the Department of Human Resources, or DIT.

Supersedes/Amends: 1403, 03/01/2013

Approved:



City Manager