

CITY OF CHESAPEAKE, VIRGINIA

NUMBER: 1.13 (11.3)

ADMINISTRATIVE REGULATION

EFFECTIVE DATE: 12/22/14

**SUBJECT: DEPARTMENT OF INFORMATION
TECHNOLOGY - ELECTRONIC DATA
RESOURCES ACCEPTABLE USE POLICY**

SUPERCEDES: 04/16/10

REVIEWED: 12/22/14

I. PURPOSE AND SCOPE

The City has made a significant investment to procure and implement information technology to enable City employees to effectively and efficiently serve its citizenry and business community. In order to maximize the availability, reliability, and efficient use of the City's information technology, it is necessary to establish guidelines for responsible use.

The purpose of this policy is to set forth rules, regulations, and restrictions for employee access and use of the City's electronic mail, Internet, Intranet, network, electronic devices (including, but not limited to, computers, Personal Digital Assistants (PDA), smart phones, cell phones and peripherals), and electronic data files (collectively referred to as "City's electronic data resources"), which will promote the preservation, protection, management and maintenance of the City's investment in its electronic data resources, while ensuring efficient service to the public. This policy also addresses the disclosure of information created, transmitted, received and stored via such resources.

This policy shall apply to all employee access or use of the City's electronic data resources, whether or not accessed by a City-owned electronic device or situated at City property.

Federal or State law may govern the matters addressed in this policy. In the event of any conflict between the relevant Federal or State law and this policy, the governing Federal or State law will control.

II. OWNERSHIP AND CONFIDENTIALITY

A. Property of the City

All components of the City's electronic data resources, including but not limited to, electronic devices and other hardware, all applications, programs and data of every kind and description created, stored or transmitted by employees using the City's electronic data resources, are the sole property of the City. EMPLOYEES HAVE NO EXPECTATION THAT ANY MATTER, DATA OR INFORMATION CREATED, STORED, PRINTED, SENT OR RECEIVED USING THE CITY'S ELECTRONIC DATA RESOURCES IS CONSIDERED PERSONAL PROPERTY.

B. Privacy/Confidentiality

All employees who use the City's electronic data resources should have no expectation of privacy or confidentiality in any information or communications created or stored on the City's electronic data resources. All data, including any stored, transmitted or printed as a document, is subject to review and audit at any time.

C. Freedom of Information Act and Privacy.

Employees should be aware that certain electronic communications using the City's electronic data resources may be subject to disclosure as "public records" under the Virginia Freedom of Information Act. EMPLOYEES SHOULD NOT HAVE AN EXPECTATION OF PRIVACY FOR ELECTRONIC COMMUNICATIONS USING THE CITY'S ELECTRONIC DATA RESOURCES.

D. Retention of records

Documents created in the performance of City of Chesapeake duties, no matter what storage media (electronic file, e-mail, paper, fax, fiche, voicemail, etc.), are governed by the Virginia Public Records Act. The Act provides that the Library of Virginia specify requirements for the classification, retention, and destruction of Public Records. Public Records of the City of Chesapeake are covered under the City's Administrative Regulation 3.07 "City Clerk's Office - RECORDS MANAGEMENT PROGRAM" which establishes the City's records management program.

III. AUTHORIZATION AND USE

Access to the City's electronic data resources imposes responsibilities, limitations and obligations upon those receiving that access. It should be clearly understood that the use of City's electronic data resources is a privilege, not a right, and may be revoked at any time, for any reason. In addition, abuse of the privilege may result in disciplinary action.

A. The use of the City's electronic data resources is permitted only with proper authorization. Any unauthorized use or attempted unauthorized use shall be promptly reported to the office of the CIO (Chief Information Officer).

B. The Department of Information Technology enables the connection of any electronic device to any of the City's electronic data resources upon receipt of a request from Department Heads, Agency Heads, Constitutional Officers, Council Appointees or their designee. City employees are not permitted to connect or attempt to connect any electronic device to the City's network without prior approval from the Chief Information Officer.

C. Employees are permitted to access the City's electronic data resources using their assigned User ID(s) and Password(s). Sharing of one's User ID(s) and Password(s) constitutes a breach of this policy and subjects the employee to disciplinary action.

D. User passwords for most systems will be chosen by the user. Users are expected to choose strong passwords that are:

- At least 8 characters long
- Changed at least once every 90 days
- Be complex with a mix of alphabetic letters, numbers and special characters (e.g., \$, #, @)
- Are not common dictionary words or proper names.

The use of strong passwords will be enforced by those systems and applications which have the technical capability to do so.

- E. Employees are permitted to read or update only such data as is authorized and required for performing their job functions.
- F. Use of the City's Electronic Data Resources and the Fair Labor Standards Act (FLSA). Individuals employed in job classifications designated as non-exempt by the Department of Human Resources who need to use the City's electronic data resources outside of their normal work schedules shall request permission to do so from their immediate supervisor prior to performing the work. Approval of such requests shall be made in accordance with departmental overtime approval procedures. The employee shall submit written documentation of hours worked to his/her immediate supervisor on the next business day after performing the work. The appropriate departmental manager shall certify an employee's written documentation of hours worked before it is submitted to payroll. Monetary payments or compensatory leave time due to an employee shall be made in accordance with established overtime provisions.

IV. ACCEPTABLE USES (Not all inclusive)

- A. Work directly related to the mission or work task of the employee's agency.
- B. To maintain currency of training or education, and/or to discuss issues related to the employee's work activities.
- C. To engage in research, analysis, and/or professional society activities related to City government work, tasks, and duties.
- D. To announce new laws, procedures, policies, rules, services, programs, information, or activities.
- E. To use electronic file folders, as necessary, to store messages or documents that may need to be retrieved later. (Employees are responsible for ensuring their electronic file folders are kept to a minimum to avoid burdening system resources.)
- F. Messages addressed to all users must be approved by the office of the CIO, and will be sent by the Department of Information Technology. Such messages will be permitted only when they are work related, apply to a majority of the recipients, and are requested by a Department Head, Agency Head, or Constitutional Officer. Examples of messages meeting the relevance test for sending to all users include, but are not limited to, the following:
 - Computer system downtime
 - Death announcements
 - Holidays and benefits information
 - Blood drives
 - Retirements
 - Street closures
- G. Personal use of the City's electronic data resources is permitted for reasonably brief periods of time, during an employee's rest or break periods or during other periods when an employee is not expected to be actively performing his/her official duties. Employees who

engage in personal use of the City's electronic data resources beyond that permitted herein may have their access revoked, and may be subject to disciplinary action.

V. PROHIBITED USES (Not all inclusive)

- A. Copying or sending copies of documents in violation of copyright laws.
- B. Making or using illegal copies of copyrighted material.
- C. Violating the laws of the U.S., the Commonwealth of Virginia or the City of Chesapeake.
- D. Sending messages containing any racist, sexist, offensive, abusive, threatening, or other inappropriate language. The city has zero tolerance for the use of such language.
- E. Conducting personal business beyond that permitted in Section IV.G above.
- F. Sending non-business mail (junk mail) to mailing lists, or to all users. Messages such as the following are considered junk mail and may not be sent to mailing lists, or to an all user mailing list:
 - Lost and found items
 - Personals
 - Items for sale
 - Pets for sale/adoption
 - Chain e-mails
 - Petitions
- G. Using the City's electronic data resources for for-profit or non-profit activities, including advertising, that are not work-related.
- H. Using the City's electronic data resources for political activities, which includes but is not limited to, soliciting votes or endorsements on behalf of a political candidate or political campaign; expressing opinions on political subjects and candidates; displaying a political picture or sign; initiating, circulating or signing a political petition; and engaging in fundraising activities for any political party, candidate or campaign.
- I. Violating any City policy.
- J. Using Internet resources to access, transmit, copy or process obscene or pornographic material.
- K. Using Internet resources to access, transmit, copy or process files dangerous to the integrity of the network.
- L. Using another person's User ID(s) and Password(s).
- M. Accessing another person's files, systems, or data without authorization.
- N. Disclosing Passwords to family members or any other person and/or allowing other persons to access any of the City's electronic data resources.
- O. Using computer programs to decode or attempt to decode Passwords or encrypted information, or to circumvent or attempt to circumvent access controls.

- P. Engaging in any activity that might be harmful or potentially harmful to the City's electronic data resources or any information transmitted by or stored therein. This includes, but is not limited to: the introduction of malicious code (e.g., creating or propagating viruses, worms, Trojan horses, etc.), disruption of services (e.g., network sniffing, pinging floods, packet spoofing, denial of service attacks, etc.), port or security scanning, or damaging files.
- Q. Altering or reconfiguring any software or hardware of the City's electronic data resources without the express authorization of the CIO.
- R. Using the City's electronic data resources to harass, intimidate, or otherwise annoy another person or group of persons.
- S. Monopolizing systems, overloading networks, or wasting computing resources (e.g., computer time, connect time, disk space, paper, etc.).
- T. Misrepresenting, under any circumstances, an employee's true identity.
- U. Developing or running personal websites on the City's electronic data resources.
- V. Copying, installing or using of any software or data files on a City electronic device in violation of any applicable copyright or license, or without authorization from the Department of Information Technology.
- W. Using the City's electronic data resources to purchase, obtain or offer products or information for City purchases except as authorized under normal City of Chesapeake Purchasing Procedures.
- X. Connecting privately owned electronic devices to the City's electronic data resources, installing personal software on any City electronic device, or loading City software on an individual's personal electronic devices without authorization of the Department of Information Technology.
- Y. Giving the impression that one is representing, giving opinions or otherwise speaking on behalf of the City or any unit of the City, unless expressly authorized to do so. Where appropriate and/or when necessary to avoid such impression, the following explicit disclaimer shall be used for communications transmitted via the City's electronic mail system: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, statement or endorsement of the City of Chesapeake."
- Z. Engaging in any other activity that does not comply with the general principles contained in this policy.

VI. ENFORCEMENT

The City considers any violation of this policy a matter of serious concern and will act to enforce the policy as follows.

A. Monitoring:

In order to assess and maintain efficiency and security, the City engages in general, system-wide monitoring of its electronic data resources, as well as any other stored or transmitted information created or received by City employees on the City's electronic data

resources. Employees should keep in mind that usage of the City's electronic data resources may be recorded, logged and stored, along with the source and destination. The City reserves the right to disclose any such information, both to City departments and to others outside the City organization, unless exempted by law.

1. The City has the right and capability of viewing employees' use and usage patterns, and to take appropriate action to maintain the security of its electronic data resources and to assure that the City's resources are being used efficiently to promote the highest levels of productivity.
2. Department Heads, Agency Heads and Constitutional Officers may request that an employee's use of the City's electronic data resources be monitored. All requests must be written and must be directed to the Chief Information Officer. Requests may be made for the following purposes and any other purposes legitimately related to the transaction of City business:
 - (a) To determine compliance with this Policy; and/or
 - (b) To evaluate the efficiency, quality or productivity of City services; and/or
 - (c) To evaluate the achievement of service goals; and/or
 - (d) To investigate any activities that are indicative of attempts to compromise the security of the City's electronic data resources; and/or
 - (e) To investigate reasonably suspected misconduct and/or violations of City policies and/or violations of law; and/or
 - (f) To comply with a law, regulation, court order or for other legitimate governmental purpose.

B. Filtering

The City utilizes content filtering software to block employee access to Internet sites when such access is: (1) not reasonably related to an employee's official duties and responsibilities; (2) inconsistent with law or City Policy; or, (3) for any other legitimate reason or concern that is inconsistent with an employee's employment responsibilities.

- C. Violation of this Policy may result in disciplinary action, up to and including termination of employment.
- D. None of the provisions of this Policy shall prevent the City from prosecuting violators to the full extent of the law.

VII. RESPONSIBILITIES

A. Employees

The City of Chesapeake regards its employees as vital frontline defenders of the integrity of the City's electronic data resources. Security of the City's electronic data resources is the responsibility of everyone associated with the City. The City therefore requires the following of employees having access to the City's electronic data resources.

1. All employees shall cooperate in the ongoing task of preserving and protecting the City's electronic data resources.
2. The Virginia Public Records Act extends to the use of mobile texting or instant messaging in the conduct of City business. Mobile phone providers do not capture mobile texting and messaging in a way that meets the retention requirements of the Commonwealth of Virginia. Therefore, it is the responsibility of the City employee to forward a copy of any text or message that is required to be retained pursuant to the Library of Virginia's records retention schedules via email or other means to a City system, such as Outlook/Exchange, for storage and retention. If such a capability is not available on the employee's mobile device, then the use of texting or messaging to conduct City business is not permitted.
3. All employees shall sign the Acknowledgment (See Attachment) that they have read and understand the City's Electronic Data Resources Acceptable Use Policy.
4. Each employee shall maintain the confidentiality of his/her assigned User ID(s) and Password(s). All employees will be held personally accountable for any and all activities logged to their User ID(s) and Password(s) on the activity logs and violation reports. Employees accept indirect responsibility for the ongoing integrity of the City's electronic data resources.
5. Each employee shall abide by and fully support this policy by encouraging compliance by fellow employees, reporting violations, and pointing out shortcomings that need to be addressed.
6. No City employee will allow any person who is not authorized to connect any electronic device to the City's electronic data resources.
7. This Administrative Regulation applies to all consultants, temporary help, and volunteers who access any part of the electronic data resources of the City. The supervising City employee, City project manager, Department Head, or Constitutional Officer who oversees such workers must ensure that they have read and agreed to the requirements of this Regulation. Violations of the requirements may result in the removal of all access rights of the worker to the City's electronic data resources.

B. Information Systems Security Analyst

The City's Information Systems Security Analyst shall fulfill the following responsibilities

1. Ensure that each user has access to this Electronic Data Resources Acceptable Use Policy; and ensure that an updated copy of this policy is maintained on the City's Intranet (CityPoint) system in the Administrative Regulations section.
2. Provide ongoing oversight of City information system security policies.
3. Ensure that this Administrative Regulation is maintained and changed as needed to conform to Federal and State law as well as to meet industry best practices.

C. IT System Security Administrators

The security administrator for each system shall fulfill the following responsibilities.

1. Add users, change user names, or change access permissions only upon written notification from the user's Department Head, Agency Head or supervising Constitutional Officer. The request must be made through the IT Help Desk (part of the NOC - Network Operation Center).
2. Delete user's access at the written request of the user's Department Head, Agency Head or supervising Constitutional Officer (The request must be made through the IT Help Desk) or according to payroll system employment termination information.
3. Provide Department Heads, Agency Heads and Constitutional Officers access to records and files maintained by any departmental employee upon request. Department Heads, Agency Heads and Constitutional Officers shall make such requests in writing to the Office of the CIO.

D. Department Heads, Agency Heads and Constitutional Officers

Department Heads, Agency Heads and Constitutional Officers shall fulfill the following responsibilities.

1. Ensure that all subordinate users abide by the guidelines set forth in this policy and other related documents.
2. Ensure that all subordinate employees acknowledge in writing that they have received, read and understand this policy. Such written acknowledgements shall be retained in employees' departmental personnel files and be made available when requested for security audits. (The failure to provide such written acknowledgements shall, not in any way, limit the City's ability to enforce this Policy.)
3. Recertify, on a yearly basis, the information system access rights and authorities of their subordinate users.

VIII. COMPLIANCE REPORTING REQUIREMENT

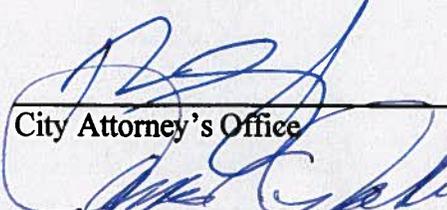
None

IX. HISTORY

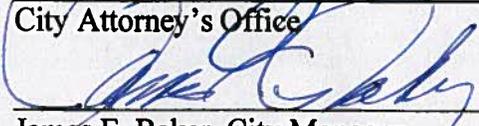
04/06/10 - This policy replaced the earlier city policy titled "INFORMATION TECHNOLOGY ELECTRONIC COMMUNICATIONS USE AND RETENTION POLICY" 05/22/2000.

X. AUTHORITY

City Manager's Office.



City Attorney's Office



James E. Baker, City Manager

12-22-2014

Date

12/22/14

Date

CITY OF CHESAPEAKE, VIRGINIA

ELECTRONIC DATA RESOURCES ACCEPTABLE USE POLICY
EMPLOYEE AGREEMENT

I hereby acknowledge that I have been provided a copy of the City's Electronic Data Resources Acceptable Use Policy. I fully understand and agree to comply with the provisions of the Policy.

I further understand that compliance with this policy is a specific condition of my continued employment with the City of Chesapeake and that my violation of this policy may subject me to disciplinary action, up to and including termination.

Employee Name – Printed

Employee's Signature

Date

Department Function Number