EXECUTIVE ORDER NO. 16

TO: **All Employees, Agencies, and Departments Under the Mayor**

FROM: **John W. Hickenlooper, Mayor**

DATE: **August 23, 2007**

SUBJECT: **Use of Electronic and Communication Devices and Services**

Purpose: This Executive Order sets forth the City's policy with regard to the appropriate use of electronic and communication devices and services provided by the City and County of Denver to its employees. "Electronic and communication devices and services" includes computers; peripherals; cell phones; pagers; PDA's; desktop phones; access to the City network, City servers, the Internet, and email; and any other electronic or communication device or service provided by the City and County of Denver.

1.0 **Applicable Authority:** The applicable authority relevant to the provisions and requirements of this Executive Order No. 16 are found in the Charter of the City and County of Denver at Section 2.2.10. Executive Order No 16, dated, June 24, 1997, Use of Electronic Mail and all Memoranda are canceled and superseded by this Executive Order.

2.0 **Policy:**

2.1 Ownership

a. The City and County of Denver provides electronic and communication devices and services to its employees to aid in the performance of City business, based on business needs determined by each City Agency and Department.

b. All electronic and communication devices and services provided by the City and County of Denver regardless of physical location or form, are considered property of the City and County of Denver and owned exclusively by the City and County of Denver.

2.2 No Expectation of Privacy

City employees who utilize electronic and communication devices and services provided by the City and County of Denver should have NO EXPECTATION OF PRIVACY when using any City-owned device or service. Employees' supervisors, Agency and Department Executive Directors, designated City Attorney's Office staff, Technology Services personnel, and any other appropriately designated City and County of Denver employee or official has the right to monitor the use of any device or service provided by the City and County of Denver to the employee, and to seize any electronic or communication device provided by the City and County of Denver to the employee.

2.3 Permissible / Prohibited Use

a. City employees shall sign the most current *Information Technology Acceptable Use Acknowledgement* prior to being given access to electronic or communication devices or services and upon any material change to the *Acknowledgement*. Users shall strictly adhere to all policies and procedures within the *Acknowledgement*, as well as any additional policies required by specific City Agencies or Departments.

b. City employees shall use assigned electronic and communication devices and services in an appropriate manner. Employees shall not knowingly transmit, retrieve or store any communication, nor intentionally visit Internet sites, that are: discriminatory or harassing; derogatory to any individual or group; obscene or pornographic; vulgar or profane; defamatory or threatening; in violation of another employee's privacy; used in order to propagate any virus, or other damaging code; used to plagiarize or copy copyright-protected material; or used for personal profit or illegal purposes; unless the employee has a legitimate business need and authorization to do so.

c. Limited, occasional, or incidental use of electronic and communication devices and services for personal, non-business purposes is permitted so long as it is of a reasonable duration and frequency, does not interfere with the employee's performance of job duties, and is not in support of a personal business.

d. All personal calls (both incoming and outgoing) made or received on a city-provided cell phone, and long distance desk phone services must be reimbursed monthly to the City and County of Denver. It is the responsibility of the employee's supervisor to ensure that personal calls have been reimbursed.

e. City employees shall not jeopardize City network security by attempting to download any music, games, pictures, video, freeware, or software from the Internet, from a received e-mail message, or from a transportable piece of media from outside the City and County of Denver.

f. City employees shall not include personally identifiable information, especially Social Security Numbers, within any unencrypted e-mail being sent outside the City's network.

2.4 Loss, Damage or Theft of a Device

a. If an electronic device provided by the City is stolen, lost or damaged, the employee must immediately notify his / her supervisor as well as the their agency Information Technology Help/Service Desk or internal IT support staff. Technology Services or the individual agency IT support staff will notify the appropriate outside vendor to suspend any existing service account.

b. In the event an electronic device provided by the City is stolen, lost or damaged, the employee will be provided one replacement electronic device at no cost to the employee. Thereafter, any damage to or loss of an electronic device must be reimbursed to the City and County of Denver. If an electronic device provided by the City is stolen, the employee must immediately notify his / her supervisor as well as their agency Information Technology Help/Service Desk or internal IT support staff. The employee must also report the theft to the appropriate police department and obtain a police report. If the device was stolen from someone's personal vehicle or home, the insurance provider should be notified and the device should be covered by that policy. Agencies and Departments may establish a different requirement or exceptions to this requirement, but must provide notice to the effected employees as such.

3.0 **Violations of the Executive Order and Discipline**

3.1 Employees may be disciplined by his/her Department for any conduct that is prohibited by or otherwise in violation of this Executive Order.

3.2 Disciplinary Action/Penalties

Violations of this Executive Order may result in suspension or termination of access to electronic and communication devices and services; disciplinary action pursuant to the City's Personnel Rules and Regulations; or legal action in the form of criminal or civil penalties.

4.0 **Memorandum Attachments:** The procedure(s) for implementing this Executive Order, may be defined by Memorandum Attachments to the Executive Order which shall become a part of the Executive Order. Further the Office of Technology Services which is responsible for the content of this Executive Order shall have the authority to issue procedural Memorandum attachments relative to this Executive Order.

Approved for Legality:

Arlene V. Dykstra
City Attorney for the City and
County of Denver

Approved:

John W. Hickenlooper
MAYOR

Turner West
Manager of Aviation

Nancy Severson
Manager of Environmental Health

Kevin Patterson
Manager of General Services

Kim Bailey
Manager of Parks & Recreation

Guillermo "Bill" Vidal
Manager of Public Works

Claude J. Pumilia
Manager of Revenue

Alvin J. LaCabe, Jr.
Manager of Safety

Roxane White
Manager of Human Services

Peter Park
Director of Planning & Development

MEMORANDUM NO. 16A

TO: **All Departments and Agencies Under the Mayor**

FROM: **Michael Hancock, Mayor**

DATE: **July 2, 2018**

SUBJECT: **Use of Electronic and Communication Devices and Services**

This Memorandum shall be attached to and become a part of Executive Order 16 Dated August 23, 2007 subject "Use of Electronic and Communication Devices and Services," and mandates the use of the attached Technology Services Acceptable Use Agreement that all employees must sign before permission is granted to use Electronic and Communication devices provided by the City.

Policy Control Information	
Department/Agency	Technology Services
Team	Information Security
Effective Date	7/2/2018
Related Policies	Executive Order 143 – Protected Data Privacy Policy Executive Order 18 – Establishment of Technology Services Executive Order 16 – Use of Electronic Communication Devices and Services Executive Order 64 – Records Management CSA Rule 16 – Code of Conduct and Discipline Policy - IT Asset Management Policy – Mobile Device Management Policy – Password Management

Purpose

This Acceptable Use Agreement supersedes all previous Acceptable Use Agreements.

The purpose of this policy is to outline the acceptable use of computer equipment at the City and County of Denver (the City), ensuring that the information created, acquired, or maintained by the City and its authorized users is used in accordance with its intended purpose and protects the employee and the City from external and internal threats; and to protect the City from inappropriate use which may expose the City to legal liability and technical risks such as virus attacks or compromise of network systems and services. This policy shall be reviewed and acknowledged on an annual basis by all City users.

Regulatory Guidance:

Regulations and Industry Standards	
CJIS	Criminal Justice Information Services
CSA CCM	Cloud Security Alliance - Cloud Controls Matrix
CSC	Critical Security Controls from Center for Internet Security
HIPAA	Health Insurance Portability and Accountability Act
NIST SP 800-53	National Institute of Standards and Technology Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
PCI - DSS	Payment Card Industry Data Security Standard

Scope

This policy applies to the following:

- All City agencies and departments, including auxiliary units and external businesses or organizations that provide information technology services to the City and County of Denver.

- All employees, civil servants, appointees, and elected officials or any other persons having access to the City's information and technology resources.
- All City technology or information resources, facility and equipment owned or leased by the City regardless of it being centralized, de-centralized, agency or department-managed.

Executive Sponsorship

Executive sponsorship for this document comes from the CIO, City and County of Denver. The CIO shall review this policy periodically with senior management to determine if changes to this policy are required.

Policy

1. General Use and Ownership

1.1. The City's protected data stored on electronic and computing devices remains the sole property of the City, whether owned or leased by the City, the employee or a third party., You must ensure through legal or technical means that protected data is secured in accordance with Technology Services Policies and Standards.

1.2. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of protected data including Personally Identifiable Information (PII), proprietary/confidential data, and regulated data.

1.3. You may access, use or share protected data only to the extent it is authorized and necessary to fulfill your assigned job duties.

1.4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.

1.5. As stated in Executive Order 16, there shall be no expectation of privacy when using any City-owned device or service. In addition, all communications conducted on the City's network are subject to the Colorado Open Records Act (CORA).

1.6. For security and network maintenance purposes, authorized individuals within the City may monitor equipment, systems and network traffic at any time, per the City's Information Security Policy.

1.7. The City reserves the right to designate authorized personnel to audit networks and systems on a periodic basis to ensure compliance with this policy.

2. Security and Protected Data

2.1. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

2.2. All personnel must lock the screen or log off when the device is unattended.

2.3. Postings by employees from a CCD email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CCD, unless posting is in the course of business duties.

2.4. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

3.1. Illegal, fraudulent or workplace inappropriate use is strictly prohibited.

Any use of the City's information and technology resources for an illegal, fraudulent or workplace inappropriate purpose or in support of such activities is prohibited. Illegal and fraudulent activities shall be defined by any violation of federal, state, or local law. Workplace inappropriate use is the use of a City information or technology resource to violate any of the rules and regulations that govern your employment or appointment to the City (*e.g.*, Municipal Code, Executive Order, Career Service Rules, Civil Service Rules and Regulations or contract).

3.2. Security and data integrity violations are strictly prohibited.

Use of the City's information and technology resources to violate security protocols, circumventing or disabling security controls, or otherwise use of the resource in an unethical manner is prohibited. Such activities include, but are not limited to: accessing accounts regardless of system for which you are not authorized or do not have a business need; copy, disclose, transfer, examine, rename, or change information, configurations, or programs not under your purview unless you are given express permission to do so by the responsible user or administrative authority; unauthorized access of another user's email or files; representing yourself as someone else, fictional or real; or using proxies or other systems to circumvent website classification or restriction; installation of any unapproved hardware devices or software; executing intentionally malicious programs or unauthorized reconnaissance/security tools.

3.3. Improper use of information is strictly prohibited.

Use of data or information created, acquired, or maintained by the City and its authorized users, in any manner other than in accordance with its intended purpose is strictly prohibited. Improper use, includes, but is not limited to: transmitting data to unauthorized endpoints; transmitting sensitive or confidential data in an un-encrypted manner, un-authorized encryption of data and failure to register the method and tokens for decryption or cipher keys with Technology Services Information Security, storing data regardless of classification on unauthorized devices or systems.

3.4. Inefficient, unnecessary or wasteful use is strictly prohibited.

Wasteful use of the City's information and technology resources includes, but is not limited to: placing programs in an endless loop; sending bulk/spam/junk mail; use of an inefficient program when efficient alternatives are available; malicious disruption of the use or performance of a computer system or network; streaming media or downloading data for

personal use that is disruptive to official business; or other use of excessive network or computational bandwidth for unofficial purposes.

3.5. Unauthorized network protocols or connections are strictly prohibited.

No personal devices are allowed on the City network unless authorized by Information Security. See the Policy and Rules of Behavior – Bring Your Own Device Usage. Only officially assigned IP addresses may be used on City managed networks. Official IP addresses may be assigned dynamically. Systems must not disguise or modify the MAC address of the network interface. Network protocols used in any manner other than in accordance with their intended purpose is strictly prohibited. Unauthorized network protocols are strictly prohibited. Technology Services Information Security must approve of all network protocols; and, any and all devices or non-City networks connected to City managed networks.

3.6. The use of unapproved executable programs is prohibited.

4. Policy Compliance

Policy Compliance will be monitored as described below. In addition to this policy, users are fully responsible for their actions and are subject to federal, state, and local laws.

4.1. Compliance Measurement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved by the Information Security team in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

1. **CCM:** Cloud Controls Matrix. A baseline set of security controls created by the Cloud Security Alliance to help enterprises assess the risk associated with a cloud computing provider. CJIS: Criminal Justice Information Systems
2. **COPPA:** The Children's Online Privacy Protection Act. The Children's Online Privacy Protection Act (COPPA) is a law created to protect the privacy of children under 13. The Act was passed by the U.S. Congress in 1998 and took effect in April 2000. COPPA is managed by the Federal Trade Commission (FTC).
3. **CSC:** Critical Security Controls. The Center for Internet Security (CIS) Critical Security Controls (CIS Controls) are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks.
4. **HIPAA:** Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

5. **NIST:** National Institute of Standards and Technology. More specifically, The City's Technology Services follows NIST Special Publication 800-53 (SP 800-53), Security and Privacy Controls for Federal Information Systems and Organizations.
6. **PCI DSS:** The Payment Card Industry Data Security Standard. A set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.
7. **Protected Data:** Per Executive Order 143, Protected Data consists of Personally Identifiable Information (PII), Regulated Data, and Proprietary and/or Confidential Information. See Executive Order 143 for the definitions of these types of protected data.

Acceptable Use Acknowledgement

By signing this acknowledgement, the user named below consents and agrees to comply with the Acceptable Use Policy. The user understands that failure to adhere to the Acceptable Use Policy may subject them to corrective or disciplinary action based on the rules and regulations that govern the user's employment or appointment to the City (*e.g.*, Municipal Code, Executive Order, Career Service Rules, Civil Service Rules and Regulations or contract), device revocation, technology resource suspension or legal action.

The user must sign this acknowledgement prior to being granted access to any City and County of Denver information or technology resource. The user must re-acknowledge any future material change to the policy. Refusal to sign this acknowledgement will result denial of access to the City and County of Denver's information and technology resources. Denial of access may hinder the user's ability to adequately perform their official duties and is not an affirmative defense for the performance issues or resulting corrective or disciplinary actions arising from the rules and regulations that govern the user's employment or appointment to the City (*e.g.*, Municipal Code, Executive Order, Career Service Rules, Civil Service Rules and Regulations or contract).

_____

User's Complete Legal Name (Printed)

_____

User's Signature

_____

City Department and Agency

_____

Date of Signature

Employee ID Number (if known)