METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

INFORMATION SECURITY POLICY

	POLICY NUMBER: ISM 1
SUBJECT: ACCEPTABLE USE OF INFORMATION TECHNOLOGY ASSETS POLICY	DISTRIBUTION DATE: 10/1/2013
	EFFECTIVE DATE: 10/1/2013
ISSUING AUTHORITY: Freddie O'Connell Executive Order No. 37	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this policy is to inform users of the Metropolitan Government's Information Technology Assets of what Information Technology uses are permissible and what uses are prohibited. Compliance with this policy drives the Metropolitan Government's ability to protect government services, government employees and the citizens of Nashville and Davidson County.

DEFINITIONS

Certain capitalized terms used in this policy have specific meanings as defined in the *Glossary* section below.

POLICY

1. Access and Use

    1.1. User Access
    All User access to Information Technology Assets:
    - shall be approved by the Department Head,
    - shall be limited to the Information Technology Assets necessary and appropriate for the User to perform the job duties and functions assigned to them.

2. Sensitive Information

    2.1. User Responsibility
    Users shall be required to know the Classification of the Information of the Metropolitan Government to which they have access, and with which they are permitted to work. Users shall understand the appropriate Security Controls that should be applied to that Information.

    2.2. Dissemination and Confidentiality
    Sending, transmitting or otherwise disseminating Sensitive Information shall be strictly prohibited unless authorized by the Department Head. Users shall not disclose or discuss any Sensitive Information with others, including friends or family. Users shall not publish or disclose any Sensitive Information to others using personal email, or to any internet sites, or through Internet blogs or social media. Users shall immediately return any documents or media containing Sensitive Information to the Metropolitan Government upon termination. User shall have no right to any ownership interest in any Sensitive Information accessed or created by the User during and in the scope of the User's work at the Metropolitan

Government. User shall maintain the confidentiality of Sensitive Information after termination of employment.

2.3. Encryption of Sensitive Information
Users shall encrypt Sensitive Information as dictated by the Director of ITS. Sensitive Information that is stored on or sent to or from Mobile Devices and Removable Media shall be encrypted while stored on the Device, while stored on Removable Media used with the Device, and during transmission to or from that Device. The User shall be required to use an Authentication Mechanism as a prerequisite to decryption of and access to the Sensitive Information.

2.4. Access from External Devices
A User shall not access Sensitive Information from a Device other than one issued to the User by the Metropolitan Government or an Approved User Owned Device. Any exceptions to this rule must be approved by the Director of ITS.

3. Security

3.1. Use of Passwords or other Authenticating Information
Users shall be responsible for keeping Authenticating Information, including passwords, private and protected. Authenticating Information shall not be printed, kept near the Device in handwritten form, stored online or shared with others, including managers or supervisors. A User shall not use an "AutoComplete" feature that allows a Device to remember User names or user id's and passwords to access Sensitive Information.

Users shall be responsible for ensuring the proper use of their account and any actions performed with a User's account shall be the responsibility of that User. Users shall not be permitted to allow other Users to have access of their Authenticating Information. Users shall not be allowed to use another User's Authenticating Information unless explicitly approved by the applicable Department Head, or as otherwise expressly required by their jobs (e.g., Metropolitan Government Information Technology Services help desk, agencies' help desks). Users shall be responsible for following all standards with regards to Authenticating Information. Immediately following these instances, the User's password must be reset.

3.2. Use of Authenticating Mechanisms such as Logical Locks
All Metropolitan Government Devices that provide access to the Network or to Sensitive Information shall employ Authenticating Mechanisms such as software that allows the Device to be locked so that access to the operating system or application requires the User to re-enter Authenticating Information. Users are required to use this software feature.

3.3. Use of Authenticating Mechanisms for Physical Access
Users shall not use physical access mechanisms (e.g., cardkey ID badges) to permit any User not similarly authorized to gain access to any secure area, i.e., piggybacking. Users shall exercise caution against another User sneaking in without the knowledge of the person providing access, i.e. tailgating.

3.4. Virus Protection
A User shall never download files from the Internet from unknown sources, open attachments to email from unknown sources, use Removable Media from unknown sources,

or otherwise risk virus infection, except where permitted by the User's Department Head or the Director of ITS. If a User has any reason to suspect material may be infected, a User shall immediately contact the Metropolitan Government Information Technology Services' help desk or the applicable Department's help desk so that the material can be virus-scanned by the Information Technology staff. Users shall not knowingly or negligently store, send or create destructive programs, including any virus, self-replicating code or any other program that operates in a similar fashion. Users shall not disable or modify the existing Metropolitan Government supported anti-virus software.

3.5. Prohibited Acts

3.5.1. Personal Use

Information Technology Assets are intended for business purposes. Users shall not access Metropolitan Government Information for personal use.

Users shall not use Information Technology Assets to engage in Internet gambling, post in non-business related chat rooms or on non-business-related Internet blogs or social media, or to view pornographic or other inappropriate material as discussed below in 3.5.2. Occasional, limited, reasonable, and appropriate personal use shall be permitted when such use does not:

- Interfere with the User's work performance;
- Interfere with any other User's work performance;
- Unduly impact the operation of Metropolitan Government and/or its Information Technology;
- Violate any law, rule, regulation, or court order; or
- Violate any provisions of this policy, or any other Metropolitan Government policy, standards or practices.

Users must use Information Technology Assets in a professional, ethical and legal manner, regardless of whether such use is personal or business–related. Access to Metropolitan Government Information shall not constitute approval of use of Metropolitan Government Information for personal use.

3.5.2. Inappropriate Material

Information Technology Assets shall not be used to upload, download, communicate, create, store, send or intentionally view, access or display material that is fraudulent, libelous, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate. The above prohibition shall not apply where such treatment of such material has been explicitly authorized by the Director of ITS and the Department of Law for the purpose of preserving evidence, or for other good reason.

Sending messages with derogatory or inflammatory remarks, including, but not limited to, remarks about race, color, national origin, gender, age, religion, sexual orientation or disability may violate federal, state or Metropolitan Government laws, rules and policies on discrimination and sexual harassment. Such messages shall not be transmitted or forwarded using Information Technology Assets except where authorized by the Director of ITS and the Department of Law for the purpose of

preserving evidence or for other good reason, or as otherwise expressly required by their job duties (e.g., law enforcement). Users encountering or receiving any such prohibited messages or material shall report the incident to a supervisor or a Department Head.

3.5.3. Intellectual Property Rights
The illegal duplication of software is strictly prohibited. Users shall not make, acquire, use or provide to others unauthorized copies of computer software. Information Technology Assets shall not be used to illegally obtain, store or copy computer software or information protected by copyright, including, without limitation, music, video, web casts, streaming media, audio content, software, designs, or other intellectual property.

3.5.4. Relocation and Modification of Information Technology Assets
Relocating or modifying Information Technology Assets including, but not limited to, network equipment, software or peripherals, shall be coordinated through the Metropolitan Government Information Technology Services Department, or the applicable Department's Information Technology staff.

3.5.5. Unauthorized System Access
The ability to read, alter or copy a file belonging to another User shall not imply permission to access that file. Use of Information Technology Assets to obtain unauthorized access to the computer systems of other individuals, companies or entities (i.e., "hacking") is strictly forbidden.

3.5.6. Proper Storage of Metropolitan Government Information
Critical Business Information shall be stored on Network drives located on Metropolitan Government supported servers or on Metropolitan Government supported cloud storage solutions that are backed up and where access to this Information can be secured. Storage of Metropolitan Government Critical Business Information to local storage on a desktop system shall be allowed when explicitly approved by the Department Head and shall be consistent with applicable data retention policies. The storage of Information of the Metropolitan Government to non-Metropolitan Government supported third-party hosted Network storage areas, such as Google Docs, Dropbox or other cloud storage mechanisms, shall not be allowed without prior approval of the Director of ITS.

3.5.7. Waste and Abuse
Users shall not monopolize or otherwise deliberately perform acts that waste, impair, damage or prevent the use by other Users of the Information Technology Assets or Information of the Metropolitan Government, or attempt to do any of the above.

3.5.8. Unauthorized Distribution of Information on the Internet
Unless specifically authorized by the Department Head, all Users shall be prohibited from making any representations pertaining to or on behalf of Metropolitan Government or from distributing or utilizing in any manner Information of the Metropolitan Government on the Internet.

3.5.9. Unauthorized Use of Assigned Information Technology Asset

Any Information Technology Asset assigned to a specific User shall only be used by that User unless explicitly approved by the User, appropriate manager, supervisor or Department Head. This provision does not include access needed for the support and maintenance of the Asset, as expressly required by a job (e.g., Metropolitan Government Information Technology Services help desk, agencies' help desk). The User's account assigned to the Asset shall only be used by the User. Any other access shall be under the authenticating credentials of the applicable User.

3.6. Reporting Of Security Incidents

Users shall report any known or suspected information technology security incidents immediately in accordance with their Department's procedures. In the absence of any defined procedures, Users shall report incidents to the appropriate management staff, such as their supervisor, who shall report it to the Metropolitan Government Help Desk. These incidents include any real or suspected event that may adversely affect the security of Metropolitan Government Information or the systems that process, store, or transmit that Information.

Examples of incidents include, but are not limited to:

- Loss or theft of computer equipment or other data storage devices and media
- Loss or theft of personally owned computer equipment, smart phone, data storage device, etc. that may store Metro information
- Unauthorized access or inappropriate disclosure of information, especially Sensitive Information, like passwords, social security numbers, credit card numbers, etc.
- Computer infected with malware
- Clicking on a link in a phishing email
- Interference with the intended use or inappropriate or improper usage of information technology resources
- Security weakness such as an un-patched vulnerability
- Inappropriate use of Metro Information Technology Assets

Failure to report a security incident immediately upon discovery of event occurrence may result in disciplinary action up to and including termination of employment.

4. Privacy

4.1. Acknowledgement of and Consent to No Expectation of Privacy

Except as otherwise provided by applicable law, Users shall not have an expectation of privacy in any Information they create store, send or receive on Information Technology Assets. Metropolitan Government retains the right, but not the duty, to monitor any and all aspects of its Information and Information Technology Assets, including, without limitation, monitoring Internet sites visited by Users, monitoring chat groups and newsgroups, reviewing materials downloaded or uploaded electronically and reviewing files, texts, chats and Email created, stored or received by a User. Such activity is to be consistent with applicable laws and performed in accordance with any Metropolitan Government policies and procedures governing these actions. Specifically, any correspondence of the Metropolitan Government in the form of email and texts may be a public record under the public records law and may be subject to public inspection. Except for the Metropolitan Government's right to retrieve and read any email message as provided in this policy, email shall be accessed only by the intended recipient. Emails and their content are occasionally visible to the Metropolitan Government

Information Technology Services Department employees or Information Technology employees of other Metropolitan Government departments engaged in routine testing, maintenance and problem resolution.

Please note that, prior to use of Information Technology, a User shall execute and enter into the *METROPOLITAN GOVERNMENT ACCEPTABLE USE OF INFORMATION ASSETS POLICY CONSENT AND RELEASE* attached hereto as *Signature Page*, which is in addition to and not exclusive of the rights granted and obligations imposed herein.

4.2. Passwords and Privacy

Use of a password does not imply that Users have an expectation of privacy in the Information they create, store, send, or receive on Information Technology Assets. The Metropolitan Government may utilize global passwords that permit access to any and all Information stored on its Information Technology Assets, regardless of whether access to that Information has been restricted by a requirement that a particular User's password be first entered. Such access may occur with or without notice to the User or the User's written consent.

5. Email Guidelines

5.1. Footer Language

Use of any email footer or signature block requires the approval of the Department Head. Users may be required by their Department Head to use an approved footer or signature block.

5.2. Mass Email Distribution

Except where necessary for legitimate Metropolitan Government business purpose, the transmission of emails to a general, non-specific audience of Metropolitan Government Users is prohibited. Requests to send emails to all Metropolitan Government employees must be approved by the Department Head, and, where necessary, by the Department of Human Resources. Requests to send Department-wide emails must be approved by the applicable Department Head.

5.3. Actions Upon Commencement of Litigation or Investigation

Automatic deletion or manual deletion by Users of emails with potentially relevant information shall be suspended to preserve responsive records once a formal investigation or litigation is reasonably anticipated or has commenced, upon receipt of a notice of litigation hold, or upon receipt of a public records request with regard to records responsive to it while it is pending. The obligation to preserve such records may be imposed by request of the Director of ITS, the Department Head, or by the Department of Law. Even in the absence of such a request, Users aware of litigation, that litigation is reasonably anticipated, or of a pending public records request should not delete any potentially relevant information.

5.4. Spoofing or Other Measures to Conceal Identity

Users shall not, under any circumstances, use "Spoofing" or other means to disguise their identities in sending email or engaging in other activities, such as altering online content, posting to blogs, social media sites, etc. Notwithstanding the forgoing, it is permissible for Users to grant “delegate” access rights to certain other Users (typically by manager to their administrative assistant).

6. At Work Network Access
   At work Network access, wired or wireless, to a Metropolitan Government supported Network, except when specifically provided for public use, shall be limited to Metropolitan Government issued and supported Devices or Approved User Owned Devices. The Department Head shall accept all responsibility for any activity or issues stemming from the use of Approved User Owned Devices. Access to Approved User Owned Devices shall be provided to Metropolitan Government IT staff when deemed necessary by the applicable Department Head. All Approved User Owned Devices connecting at work to the Network shall meet Metropolitan Government ITS minimum security requirements and Users shall maintain their Approved User Owned Devices' security on an ongoing basis.

   At work Network access, wired or wireless, to a Metropolitan Government supported Network designed for public use shall not be used by Metropolitan Government Users during work hours, including breaks and lunch times. The public use Network is meant to provide services to the public. Use of the public Network shall be limited to intended purpose.

7. Permitted Forms of Remote Access
   External access into the Network shall utilize a Metropolitan Government approved Virtual Private Network (VPN) or similar remote access solution, except for Information Technology Assets specifically configured for external access, such as applications accessible outside the Network, email, Metropolitan Government approved cloud hosted services, etc. Dial-up access, remote PC connection applications such as, LogMeIn, PC Anywhere, GoToMyPC, etc., are not allowed. Any built-in remote assistance functionality, such as Microsoft remote assistance, shall require request approval by the User and constant monitoring by the User during the session. All requests for remote access into the Network shall be approved by the User's supervisor and the User's Department Head.

8. Removable Media
   Users shall only use Removable Media that has been supplied by the Metropolitan Government. Any Removable Media that is used for the storage of Sensitive Information shall be encrypted with encryption software approved by the Metropolitan Government ITS Department. The User shall return the Removable Media to the issuing Department consistent with Departmental requirements.

   8.1. Physical Security
   Removable Media shall be secured if not in the possession of the User. Removable Media taken off-site and in transit shall not be left unattended. The theft or loss of any Removable Media containing Sensitive Information shall be reported immediately to the User's Department Head.

   8.2. Information Storage
   Users who store Information of the Metropolitan Government on Removable Media shall first ensure that they are fully aware of the content and Classification of that Information.

9. Destroying Information When No Longer Needed
   Information of the Metropolitan Government stored on any of the following Devices shall be removed using a Metropolitan Government ITS approved method: hard drives, CDs, DVDs, copiers, computer memory, flash drives, etc., This should be done prior to the Device being retired or disposed of, and in a manner that is consistent with applicable laws and a records retention schedule approved by the Davidson County Public Records Commission, including, without limitation, the

General Records Schedule of the Metropolitan Government of Nashville and Davidson County. *See also*, the provisions of paragraph 5.3, above, regarding pending public records requests, or where litigation has commenced or is reasonably anticipated.

10. Approved Mobile Devices

Any Mobile Device, such as a mobile phone, tablet, etc., that will be used to store or access Information of the Metropolitan Government shall be managed using a Metropolitan Government approved mobile device management and mobile application management solution for Metropolitan Government provided devices and mobile application management solution for non-Metropolitan Government devices. These Devices are required to be PIN protected and shall allow remote wiping of any Metropolitan Government Information in the event of theft or loss of the Device. The theft or loss of any Mobile Device used to store or access Information of the Metropolitan Government shall be immediately reported to the User's Department Head.

11. Social Media and Social Networking

Social media consists of Internet-based applications including web- and mobile-based technologies that allow for the creation and exchange of user-generated content. Examples of social media include, but are not limited to, Facebook, blogs, Twitter, Instagram, TikTok, LinkedIn, YouTube, and comments following online news articles. Social networks are communities of people or organizations that share interests and/or activities and use a wide variety of Internet technology to interact. The Metropolitan Government of Nashville and Davidson County uses social media and social networking as means of communicating its services, events, and performance to the public.

11.1. Departmental Use of Social Media

An employee must be authorized by the Department Head or designee to represent the Department prior to authoring content on a Department's social media. Employees representing the Metropolitan Government Department through social media will conduct themselves as a representative of the city. The Metropolitan Government's and the Department's rules, policies and standards of conduct apply to city employees who engage in social media/networking activities while conducting city business.

Metro Government's social media content and administration of social media sites shall follow *Metro's Departmental Use of Social Media* standard.

11.2. Employee Personal Use of Social Media

In general, employees who participate in social media and social networking are free to publish their own personal information without censorship by the Metropolitan Government. Employees who choose to identify themselves as the Metropolitan Government employees through social media must state in clear terms that their expressed views are theirs alone and do not reflect the views of the Metropolitan Government. Except as authorized, employees are prohibited from representing the Metropolitan Government through their personal use of social media.

Just as employees' behavior outside of work could constitute a failure of good behavior which reflects discredit upon themselves, the Department and/or the Metropolitan Government, their contribution to social media and social networking can do the same. In situations where an employee's social media contribution causes an issue which is substantially related to an important government interest, or which has the effect of creating a disruption in the workplace (e.g., such as where the usage is tied to threatening, discriminatory, harassing, or

retaliatory behavior directed at the Metropolitan Government or an employee of the Metropolitan Government), disciplinary action up to and including termination may be merited.

Except where authorized, employee's social media content will not include Intellectual property of the Metropolitan Government (e.g., drawings, designs, software, ideas and innovation) or the Metropolitan Government's logo.

12. Out of Country Travel
    Metropolitan Government Information Technology Assets, including, but not limited to, smartphones, laptops, USB storage devices, shall not be taken to any country under a Level 2 or above Travel Advisory as defined by the United States Department of State. Any Removable Media taken outside United States jurisdiction, regardless of destination, shall not store any Critical Business Information or Sensitive Information. Loss of any Metropolitan Government Information Technology Assets for any reason, including confiscation, shall be reported as a security incident. Use of any Metropolitan Government Information Technology Assets outside United States jurisdiction must follow all applicable Metropolitan Government policies.

13. Miscellaneous
    This policy shall supersede all previous Metropolitan Government acceptable use policies including but not limited to the "Comprehensive Internet and Electronic Mail Use Policy" formerly attached to Mayor Dean's Executive Order 15. This policy may be amended or revised at any time. Users are responsible for periodically reviewing this policy for any revisions and for adhering to those revisions. This policy does not supersede any Departmental policies that address areas not defined in this policy as long as the requirements of such Departmental policies equal or exceed the minimum requirements set forth in this policy. This policy does not waive the User's responsibility to follow all applicable legal and/or regulatory requirements. Violation of this policy may result in disciplinary action up to and including termination of employment.

GLOSSARY

Approved User Owned Devices – any Device owned by a User, where connection to the non-public Network by the User using that Device has been approved by the User's Department Head. SOURCE: Acceptable Use Policy Work Group

Authenticating Information – any information that can be used to verify the identity of a User, process, or Device, often as a prerequisite to allowing access to resources in an information system, such as passwords, PINs, fingerprints, etc. SOURCE: NIST SP800-43

Authentication Mechanism – hardware or software-based mechanisms that force Users, Devices, or processes to prove their identity before accessing data on an information system, such as encryption software, smart cards, fingerprint readers, etc. SOURCE: CNSSI-4009

Classification – the security classifications of Information as provided in the *Metropolitan Government Information Classification Policy*. SOURCE: Metro Legal

Critical Business Information – vital Information, without which Metropolitan Government could suffer serious financial, legal or other damages or penalties and/or incur a disruption of services. SOURCE: Acceptable Use Policy Work Group

Department - Metropolitan Government department, agency, office or board by which the User is employed. SOURCE: Metro Legal

Department Head - the applicable director, appointing authority, elected official, or other Department Head of the Department or agency in which the User is employed, or their designee. SOURCE: Metro Legal

Device – computing and communications hardware with information storage capability (e.g., computers, servers, PDAs, cellular telephones, smart phones) SOURCE: Acceptable Use Policy Work Group

Director of ITS – the Director of the Department of Information Technology Services of the Metropolitan Government. SOURCE: Acceptable Use Policy Work Group

Information – Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. SOURCE: CNSSI-4009

Information Technology Assets - all electronic devices, communication and information systems and similar technology (as listed below), owned, leased or licensed by Metropolitan Government and provided to Users for their use in connection with, or concerning, business of the Metropolitan Government, including, without limitation:

- Network access, wired or wireless, both local and internet
- Computer hardware, Devices, network equipment, telephones, printers, copiers, and fax machines, calculators, Removable Media, etc.
- Software, intellectual property, operating systems, firmware, source code, applications, middleware, etc.
- Storage solutions, including cloud-based, removable storage, Storage Area Networks, etc.

- Procedural Information, configuration, or documentation of any of the above

SOURCE: Acceptable Use Policy Work Group

Logical Locks - The prevention of User access to data that is provided by software, as opposed to physical locks. SOURCE: NIST SP800-43

Mobile Devices - Portable Devices (e.g., tablets, notebook/laptop computers, PDAs, cellular telephones, digital cameras, smart phones and audio recording Devices). SOURCE: Acceptable Use Policy Work Group

Network – Metropolitan Government supported Network, comprised of information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control Devices, and the Information Technology Assets and Information of the Metropolitan Government that that infrastructure supports. SOURCE: Acceptable Use Policy Work Group

Personal Identification Number (PIN) – An alphanumeric code or password used to authenticate an identity. SOURCE: FIPS 140-2

Removable Media - Storage media which is designed to be removed from the computer without powering the computer off. This includes, but is not limited to, DVDs, CDs, memory cards, floppy disks, zip disks, tapes, USB flash drives, External hard disk drives. SOURCE: Acceptable Use Policy Work Group

Security Controls - Management, operational, and technical measures prescribed for an IT system which, taken together, satisfy the specified security requirements and protect the confidentiality, integrity, and availability of the system and its information. SOURCE: NIST SP800-43

Sensitive Information - Any Information of the Metropolitan Government classified as "Confidential" or "Restricted" as defined by the *Metropolitan Government Information Classification Policy*. SOURCE: Acceptable Use Policy Work Group

Spoofing – 1. Faking the sending address of a transmission to gain illegal entry into a secure system. 2. The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating masquerading, piggybacking, and mimicking are forms of spoofing. SOURCE: CNSSI 4009

User - All Metropolitan Government employees, independent contractors, consultants, temporary or part-time employees, leased employees, interns, and other persons or entities to whom Metropolitan Government has explicitly granted access to Metropolitan Government's Information Technology Assets and Information. SOURCE: Acceptable Use of Information Technology Assets Policy Work Group; Confidential Agreements Work Group

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov

REFERENCES

ISO 27002: sections 7.1.3, 10.8, 11.7.1

NIST Special Publications 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations*: AC-1, AC-6, AC-20, PL-4, MP-4, MP-6,
NIST Special Publications 800-45, *Guidelines on Electronic Mail Security*
NIST Special Publications 800-88, *Media Sanitation Guide*
NIST Special Publications 800-46, *Guide to Enterprise Telework and Remote Access Security*
CNSSI Instruction No. 4009 26 April 2010, *National Information Assurance (IA) Glossary*
FIPS 140-2, *Security Requirements for Cryptographic Modules*
Metropolitan Government Information Classification Policy
Criminal Justice Information Services (CJIS) Security Policy ver. 6.0
NIST Cybersecurity Framework ver. 2.0
NIST Special Publication 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
Payment Card Industry Data Security Standard version 4.0.1

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	5/3/2011	First released version.
1.1	9/15/2011	Added “Department” and “Employee Number” fields to METROPOLITAN GOVERNMENT ACCEPTABLE USE OF INFORMATION ASSETS POLICY CONSENT AND RELEASE form.
1.2	10/28/2011	Added “Except as otherwise provided by applicable law” and “except where it would be prohibited by law” to the METROPOLITAN GOVERNMENT ACCEPTABLE USE OF INFORMATION ASSETS POLICY CONSENT AND RELEASE form.
1.3	1/8/2013	Added to Section 6 wording covering access to public network; added new Section 11 to cover “Social Media and Social Networking”.
1.4	10/1/2013	Annual review and update.
1.5	4/10/2015	• 2.2 Dissemination was renamed to Dissemination and Confidentiality with language added to address confidentiality and to build in some NDA language into the AUP. • Section 3.3 was added to address concerns around "piggybacking." • In section 3.5.1 Personal Use, the section, "with prior authorization from the applicable Department Head and..." was removed. • 3.5.4 Relocation and Modification of Equipment was renamed to Relocation and Modification of Information Technology Assets • The term "tablets" was added to the definition of "Mobile Devices" to better reflect current IT offerings.
1.6	3/2/2018	Added section 3.6 Reporting of Security Incidents
1.7	5/1/2018	Modification to section 11.1 to reference Metro’s *Departmental Use of Social Media* standard.

1.8	5/11/2023	Update ISSUING AUTHORITY to "Reaffirmed via John Cooper Executive Order No. 001" 2.2 Replaced "sites such as Facebook or Twitter" to "social media." 3.3 Added specific mentions of "piggybacking" and "tailgating". 3.5.1 Added "Users shall not access Metropolitan Government Information for personal use. " 3.5.6 Added "Metropolitan Government supported cloud storage solutions" to address use of cloud storage solutions. 3.5.9 Added *Unauthorized Use of Assigned Information Technology Asset* and text. 4.1 Added "and texts" to clarify the scope of this section. 7. Added "Metropolitan Government supported cloud storage solutions" and replaced "Skype" with "Teams. 10. Updated language in header from "Cell Phones, PDAs or Blackberries" to "Mobile Devices". Updated language to include use of Metro approved mobile device management and mobile application management solution. Addition of 12. *Out of Country Travel* heading and text GLOSSARY: "Information Technology Assets" added the follow bullet points: • "Network access, wired or wireless, both local and internet • Storage solutions, including cloud based, removable storage, Storage Area Networks, etc."
1.9	8/29/2025	Update ISSUING AUTHORITY to "Reaffirmed via Freddie O'Connell Executive Order No. 37" Change to reference to reflect new administration Change to reflect use of rev 5 of NIST 800-53 as a reference Change to reflect use of rev 2 of NIST Cybersecurity Framework Change to reflect use of version 6 of CJIS as a reference Change to reflect use of version 4.01. of PCI-DSS as a reference

METROPOLITAN GOVERNMENT
ACCEPTABLE USE OF INFORMATION ASSETS POLICY

CONSENT AND RELEASE FORM

I, _____, as an employee of/applicant for employment with Metropolitan Government, acknowledge that I have read and understand the Metropolitan Government's *Acceptable Use of Information Technology Assets Policy.* Except as otherwise provided by applicable law, I have no expectation of privacy when using the Metropolitan Government's Information Technology Assets

I acknowledge that Information may be gathered through monitoring, searching and reviewing my or any use of the Metropolitan Government's Information Technology Assets and Information, including, without limitation, files and emails. I understand that, except where it would be prohibited by law, the Metropolitan Government may disclose any Information obtained through such monitoring and I consent to such disclosure. I understand that such information may be used in a disciplinary action against me or in judicial proceedings. I understand that any violations of this Policy on my part could result in disciplinary actions being taken against me, up to and including termination of employment.

_____
Employee/Applicant Signature

_____
Date

_____
Employee Number

_____
Department

Form Version 1.2