Topic: Citywide Cybersecurity Program Policies & Standards	**No**: P-02-PR-AT
CSP Function: Protect **CSP Category**: Awareness & Training	**Issuance Date:** 05/20/2025
Title: Citywide Cybersecurity User Responsibility Policy	**Standard Classification:** Non-Restricted **Issued By:** NYC Cyber Command **Contact Info**: CyberPolicies@oti.nyc.gov

Revision History:

Version	Description of Change	Approver	Issuance Date
1.3	Page 1, paragraph 4: "Confidential Agency or citizen data" changed to "Agency Data." Page 1, paragraph 4b: "Paper documents must be filed and stored in a locked device when not in use" was changed to "Documents classified as PRIVATE or CONFIDENTIAL must be filed and stored appropriately when not in use.	DOITT	05/05/2010
1.4	Updated header with new NYC logo and added this revision history table to the document.	DOITT	06/16/2011
1.5	Added the following text: Passwords used by a person on City of New York systems should be different from any passwords used by the same person on non-City of New York systems (for example, on accounts used on social networking, ecommerce, and other personal online sites). In the event that a personal (non-City) account password is compromised, this reduces the risk to City systems.	DOITT	11/29/2012
1.6	Policy review and minor formatting updates.	DOITT	09/09/2014
2.0	Reformatted document to new NYC Cyber Command policy Template. Updated document with new OTI logo. Added requirement to report suspected incidents and phishing emails to the SOC. Added requirements to label and handle data according to its classification. Changed term from PRIVATE or	Kelly Moan, (NYC CISO)	05/20/2025

	CONFIDENIAL to “Restricted” or “Sensitive” to match current *Citywide Data Classification Policy*. Removed reference to Fax and PDA devices. Modified password requirements to match the updated *Citywide Password Management and the Citywide Password Management Standard.* Added requirements for users to not use any AI tools that have not been approved by their Agency CISO. Added requirement for users to complete cybersecurity awareness training in accordance with the *Citywide Cybersecurity Awareness Training Policy.* Added requirement that upon end of employment or conclusion of contract including returning city-owned Devices, access cards, and “Restricted” or “Sensitive” Data, ceasing and not attempt to access any City Data or City Systems or transfer or retain any data after their access has been removed or modified.		

Table of Contents

1.0 Purpose

1.1. The purpose of the *Citywide Cybersecurity User Responsibility Policy* is to establish the requirements for users accessing City Systems, City Data, City Assets and uphold the confidentiality, integrity, and availability of City Data and City Systems.

1.2. This Policy defines the appropriate use of City Systems, City Data, and City Assets.

1.3. This Policy is issued in furtherance of the Citywide Cybersecurity Program (the "Citywide CSP").

2.0 Scope

2.1. This Policy applies to all Users who access, uses, or manage City System, City Data, and City Assets. This includes, but is not limited to employees, contractors, and consultants performing work for the Agency. Each Agency is responsible for adherence to this Policy.

2.2. This policy applies to all Agency Systems. An Agency System includes:

2.2.1. All Systems owned, maintained, or operated by or on behalf of an Agency.

2.2.2. All Systems that connect to a City-owned Network.

2.2.3. All Systems that create, process, access, store, transfer or destroy City Data.

2.2.4. All Systems that support the City's delivery of services to the public.

2.2.5. All Systems utilized to support or enable the City assigned mission and duties, to protect City Data, to fulfill its legal responsibilities, and to protect individuals.

3.0 Requirements

3.1. Agencies must ensure that all City employes, contractors, consultants, and vendors adhere to the following user responsibilities outlined in this *Citywide Cybersecurity User Responsibility Policy (P-02-PR-AT).*

3.1.1. Users must comply with Citywide Cybersecurity Policies and Standards.

3.1.2. Users must ensure they follow all requirements of this Policy when working remotely.

3.1.3. Users must immediately report any suspicious or anomalous behavior that may indicate a potential threat or suspected Cybersecurity Incident to the 24/7 NYC Cyber Command Citywide Security Operations Center at +1 718-403-6761.

3.1.4. Users must report suspected phishing emails or social engineering attempts by using the

City's reporting button or contacting the NYC Cyber Command Citywide Security Operations Center directly.

3.1.5. Users are responsible and accountable for safeguarding City Systems, City Data, and City Assets from unauthorized access, modifications, disclosure, and destruction.

3.2. Access Control and Data Classification Requirements

3.2.1. Users must only access City Data to which they have been given authorized access and must ensure that City Data is only shared with those that have authorized access, and a business need to know in the performance of their duties.

3.2.2. Users must familiarize themselves with the *Citywide Data Classification Policy (P-03-PR-DS)* and *Citywide Data Classification Standard (S-03-PR-DS)* and ensure that City Data is labeled with the appropriate classification type.

3.2.3. Users must ensure that City Data is handled in accordance with its classification and uphold the requirements established in the *Citywide Information Management Policy (P-ID-RA-02)*, and *Citywide Information Management Standard (S-ID-RA-02).*

3.2.4. Users must ensure that City Data classified as "Sensitive" or "Restricted" is only stored on authorized Devices, Systems and Removable Media that comply with the minimum encryption requirements outlined in the *Citywide Encryption Policy (P-02-PR-DS)* and *Citywide Encryption Standard (S-02-PR-DS).*

3.2.5. User must utilize approved secure transmission methods when handling "Sensitive" or "Restricted" City Data as required by the *Citywide Information Management Standard (S-ID-RA-02)*. The use of unapproved or unsecure methods for transmitting Sensitive" or "Restricted" City Data is prohibited.

3.2.6. Users must not remotely access City Systems and City Data until they have been authorized and granted management approval as required by the *Citywide Remote Access Policy.*

3.3. Clean Desk Policy and Automatic Lock Screen

3.3.1. All physical documents containing "Sensitive" or "Restricted" Data must be locked and not be stored where it can be easily accessed. Examples of "Sensitive" or "Restricted" Data include proprietary/technical information, internal audit findings, or any material containing Personally Identifiable Information (PII). For more examples, please refer to the *Citywide Data Classification Policy (P-03-PR-DS)* and *Citywide Data Classification Standard (S-03-PR-DS).*

3.3.2. Physical documents include but are not limited to printed and handwritten documents that contain City Data.

3.3.3. All physical documents designated as "Restricted" or "Sensitive" being hand-delivered, printed, or physically transported must be kept with the authorized individual and

protected from unauthorized disclosure.

3.3.4. Workstations, City-owned Devices and any electronic equipment used to access, process, store, or transmit City Data must be locked when not in use or when the user has stepped away from their workstation.

3.3.5. Physical documents containing "Sensitive" or "Restricted Data" must be shredded before disposal.

3.3.6. Before disposing of Removable Media, Users must contact their Agency IT department to ensure proper disposal as required by the *Citywide Cybersecurity Requirement for the Re-use and Disposal of Systems and Non-Computing Devices Policy (P-04-PR-DS)*.

3.3.7. User must follow clean desk principles when working remotely.

3.3.8. Users must log off at the end of the workday.

3.4. Technology Acceptable Use

3.4.1. City-owned Devices must be used only for authorized purposes. Users must refrain from using City resources for personal use and for activities that are unauthorized consistent with the City of New York Policy on Limited Personal Use of City Office and Technology Resources, their Agency's Acceptable Use Policy, applicable laws, rules, or regulations.

3.4.2. City-issued email addresses may only be used for official, professional, City job-related websites. Users must not input City Data into accounts that have not been approved for work purposes and must not use City-issued email addresses for subscribing or registering for online personal accounts, personal subscriptions, or personal online sales accounts.

3.4.3. Users are prohibited from using City-owned Devices to sign into web browsers using a personal account or taking any actions that would cause City Data and metadata to be synchronized to external, non-city/agency owned accounts.

3.4.4. Users are responsible and accountable for safeguarding and preventing the unauthorized disclosure, modification or destruction of City Assets entrusted in their care.

3.4.5. Users must not store, transmit, or process City Data using third-party platforms or services without approval from their Agency CISO or their designee.

3.4.6. Any attempt to bypass or disable security controls is prohibited (e.g., disabling antivirus software, or creating unauthorized network connections).

3.4.7. Users are responsible for securing their assigned City-owned Devices, including protecting them from theft, loss or unauthorized physical access. Loss of City-owned Devices must be reported to the User’s supervisor and follow their agency’s reporting

protocols for lost Devices.

3.5. Prohibited Usage of Software

3.5.1. Users must not install or use unauthorized or illicitly acquired software on any City Systems as required by the *Citywide Cybersecurity Inventory and Control of Software Policy (P-03-ID-AM)*.

3.5.2. Users must not share credentials to gain access to any software and bypass authorization in accordance with the *Citywide Anti-Piracy and Credential Misuse Policy (P-03-PR-IP)*.

3.5.3. Users must not install any browsers plugs-ins not explicitly authorized by the Agency.

3.5.4. Users must not connect City Systems or City Assets to any network not authorized by their Agency. Users are strongly encouraged to not connect to insecure network. (e.g., public Wi-Fi).

3.5.5. Users must only store and process City Data in applications that have been authorized by the Agency.

3.5.6. Users must not use any AI tools, including software, application, or web-based tools, that have not been approved by the Agency CISO and authorized for use by the Agency as required by the *Citywide Cybersecurity Usage and Development of Artificial Intelligence Systems Policy (P-08-PR-DS).*

3.5.7. Users must not input City Data, including metadata or synthesized summaries, into AI tools or chatbots that have not been explicitly approved for use by the Agency and for the user.

3.5.8. Users must not uninstall City-installed software.

3.6. Cloud Storage Usage

3.6.1. Users must not upload City Data to cloud storage solutions that have not been reviewed by the Agency CISO and approved for use by the Agency.

3.7. Bring Your Own Device (BYOD) - Use of Personal Devices to Access City Networks

3.7.1. Users must not use personally owned Devices to access or to store City Data unless the personal device is compliant with the requirements of the *Citywide Mobile Computing Device Policy* and has been authorized for use and approved by the Agency CISO per the *Citywide Cybersecurity Inventory and Control of Systems Standard (S-02-ID-AM).*

3.8. Password Requirements

3.8.1. Users are responsible for following the password requirements for users outlined in the *Citywide Password Management Standard (S-03-PR-AC)* and implemented by their

Agency.

3.8.1.1. To support good security practices, Users must ensure that their passwords are unique to each of their accounts. Users must refrain from constructing password and passphrase from anything easily identifiable or associated with the user or the Agency such as, Agency-specific terms, phrases, or personal information (e.g., such as name, work telephone, etc).

3.8.1.2. Users should not use "Password Hints". If an application requires a password hint, Users must not use their actual password/passphrase as their hint, instead, generic words, or words that cannot easily lead to guessing the password or passphrase, must be used.

3.8.1.3. Users must only store passwords in open-source and/or browser-based password manager solutions that have been approved by the Agency CISO or equivalent as outlined in the *Citywide Password Management Standard (S-03-PR-AC).*

3.9. Password Confidentiality

3.9.1. Passwords and PINs must never be shared except when approved to be shared with an authorized user. When passwords must be shared, it must be done using an approved secure method.

3.9.2. Users must never write down passwords and PINs whether physical or electronically, this is to prevent data loss and unauthorized access.

3.9.3. Users must not display passwords and PINs on screen except when securely entering them as part of an authentication process. In order to prevent data loss, any display beyond what is strictly necessary is prohibited.

3.9.4. Users must report to their supervisor, Agency CISO or equivalent, and the NYC Cyber Command Citywide Security Operations Center if they suspect or know of any passwords or PINs that have been compromised. The password or PIN must be changed.

3.10. Privacy Considerations

3.10.1. City-owned Devices and Removable media are the property of the City of New York. Users have no expectation of privacy when using City devices and networks. Content and traffic on CityNet and Devices connected to CityNet may be monitored and reviewed.

3.11. Cybersecurity Awareness and Training

3.11.1. Users are responsible for completing the Cybersecurity Awareness Training in compliance with the *Citywide Cybersecurity Awareness Training Policy (P-01-PR-AT)*.

3.12. Asset Returns and User Access Revocation

3.12.1. Users must return all City Assets upon termination of employment or contract. This includes but is not limited to; City-owned Devices, access cards, copies of information received and/or created.

3.12.2. User accounts to City Systems, City Data, and City Assets must be deprovisioned immediately upon termination of employment, completion of contract, or conclusion of the business relationship.

3.12.3. Users must not copy, transfer, or retain any City Data after their access to City Systems, City Data and City Assets has been revoked or modified.

3.12.4. Users found to be in violation of Citywide Cybersecurity Policies and Standards may have their City Systems and/or City Data access suspended or revoked as determined by their supervisor and/or the Agency CISO or designee.

3.13. Acknowledgement

3.13.1. Users of City Systems, City Data and City Assets will receive a copy of the *Citywide Cybersecurity User Responsibility Policy (P-02-PR-AT)* and must sign an acknowledgement of receipt and understanding.

4.0 Roles and Responsibilities

4.1. Agency Head

4.1.1. Responsible and accountable for the implementation of the Citywide CSP, including this Policy.

4.1.2. Responsible for the enforcement of this Policy within its Agency.

4.1.3. Responsible for the enforcement of this Policy with regard to all personnel, employees, contractors, and consultants performing work for the Agency.

4.1.4. Responsible for the development and implementation of adequate controls enforcing this Policy within its Agency.

4.1.5. Responsible for periodically reviewing that policies and controls are effectuated to reflect changes in Policy requirements.

4.1.6. Responsible for ensuring all personnel understand their responsibilities in accordance with this Policy and related standards within its Agency.

4.1.7. Responsible for ensuring compliance with any applicable laws and regulations that its Agency must comply with. If requirements within this Policy contradict any applicable laws and regulations with which its Agency must comply, the Agency is responsible for complying with the requirements mandated by the applicable laws and regulations and

notifying NYC Cyber Command of the conflict.

4.2. NYC Cyber Command

4.2.1. Responsible for establishing the information security policy and standards for Agencies.

4.2.2. In accordance with the *Citywide Cybersecurity Audit Policy Charter (C-02-ID-GV)*, NYC Cyber Command is responsible for auditing Agencies for compliance with this Policy.

4.2.3. Responsible for notifying the New York Chief Technology Officer ("NYC CTO") of material non-compliance with this Policy by an Agency.

4.2.4. Responsible for the implementation of the controls set forth in this Policy within its organization.

4.2.5. Responsible and accountable for the implementation of this Policy on System(s) it owns and/or operates.

5.0 Authority

5.1. This Policy is issued pursuant to the Citywide CSP, and the authorizations and authorities cited therein.

6.0 Enforcement

6.1. Users should be aware that unauthorized use of City of New York assets may result in disciplinary action.

6.2. Each Agency Head possesses primary responsibility and accountability for enforcing this Policy and any related policy and standards within its Agency.

6.3. In accordance with the Citywide CSP and consistent with Cyber Command's authority and obligations under the NYC Charter, NYC Mayoral Executive Order 10 of 2020, and Section 6.3 of the Citywide CSP, Cyber Command shall promptly notify the NYC CTO when it becomes aware of any Agency's material non-compliance with the requirements of this Policy.

6.4. City employees who are responsible and accountable for the execution of and compliance with this Policy may be subject to disciplinary action, as well as criminal or civil liability, for violating the security requirements of this Policy.

6.5. Any Agency that does not comply with this Policy may have non-compliant System(s) and Device(s) taken offline until such time that a formal assessment can be performed at the discretion of NYC CISO and may be subject to further action the NYC CTO deems necessary

to maintain the City's Networks and Systems security.

6.6. NYC Cyber Command may conduct periodic audits to review compliance with this Policy and supporting documents.

6.7. NYC Cyber Command may withhold approval for any cybersecurity-related spending request by Agencies not in compliance with this Policy.

7.0 Definitions

7.1. Below are the defined terms used in this Policy. Current definitions for defined terms can be found in the Citywide Cybersecurity Program (CSP) Glossary.

7.1.1. Agency
7.1.2. Agency Chief Information Security Officer ("Agency CISO")
7.1.3. Agency Head
7.1.4. Agency Network(s)
7.1.5. Agency System
7.1.6. Applications
7.1.7. Citywide Cybersecurity Program (CSP)
7.1.8. City
7.1.9. CityNet
7.1.10. Asset(s)
7.1.11. City Data
7.1.12. City Systems
7.1.13. Cybersecurity Incident
7.1.14. User(s)
7.1.15. Personal Account
7.1.16. Removable Media
7.1.17. System(s)
7.1.18. Device(s)
7.1.19. Citywide Security Operations Center
7.1.20. NYC Cyber Command
7.1.21. Password(s)

8.0 References

8.1. Citywide Cybersecurity Program, Version 1.0. (October 2019).

8.2. Citywide Cybersecurity Audit Program Charter (C-02-ID-GV).

8.3. Citywide Cybersecurity Program (CSP) Glossary.

8.4. City of New York Policy on Limited Personal Use of City Office and Technology Resources

8.5. NIST Cybersecurity Framework Version 2.0 (March 2024).

8.6. NIST Special Publication (SP) 800-53, rev. 5, Recommended Security Controls for Federal Information Systems (December 2020).

8.7. NIST Special Publications (SP) 800-12, rev.1, An Introduction to Information Security (June 2017).

8.8. CIS Critical Security Controls, Version 8 (April 2021).

8.9. NISTIR 7298 Rev. 3, Glossary of Key Information Security Terms (July 2019).

9.0 Related Citywide Policies and Standards

9.1. Citywide Data Classification Policy (P-03-PR-DS)

9.2. Citywide Data Classification Standard (S-03-PR-DS)

9.3. Citywide Information Management Policy (P-ID-RA-02)

9.4. Citywide Information Management Standard (S-ID-RA-02).

9.5. Citywide Encryption Policy (P-02-PR-DS)

9.6. Citywide Encryption Standard (S-02-PR-DS).

9.7. Citywide Remote Access Policy.

9.8. Citywide Cybersecurity Requirement for the Re-use and Disposal of Systems and Non-Computing Devices Policy (P-04-PR-DS).

9.9. Citywide Anti-Piracy and Credential Misuse Policy (P-03-PR-IP).

9.10. Citywide Cybersecurity Usage and Development of Artificial Intelligence Systems Policy (P-08-PR-DS).

9.11. Citywide Mobile Computing Device Policy

9.12. Citywide Cybersecurity Inventory and Control of Software Policy (P-03-ID-AM).

9.13. Citywide Cybersecurity Inventory and Control of Systems Standard (S-02-ID-AM).

9.14. Citywide Password Management Standard (S-03-PR-AC)

9.15. *Citywide Cybersecurity Awareness Training Policy (P-01-PR-AT)*