Cyber Command

Topic: Citywide Cybersecurity Program Policies & Standards	**No:** P-ID-RA-02
CSP Function: Identify **CSP Identify Category:** Risk Assessment	**Effective Date:** 10/23/2019
Title: Citywide Information Management Policy	**Policy Classification:** Non-Restricted
	Issued By: NYC Cyber Command ("NYC3") **Contact Info:** Policies@cyber.nyc.gov

Revision History:

Version	Description of Change	Approver	Date
1.1	Initial version released	Geoff Brown	2/13/2019
1.2	Changes Policy to conform to Citywide Cybersecurity Program. Separates information classification from information management. Reformats document to new NYC3 Policy Template.	Geoff Brown	10/23/2019

Table of Contents

1.0 Purpose

1.1 This policy is issued in furtherance of the Citywide Cybersecurity Program (the "Citywide CSP").

1.2 This policy establishes a requirement for Covered Organizations to protect and manage all City Information processed, stored or transmitted on Systems owned, maintained or operated by or on behalf of a Covered Organization thereof.

1.3 This policy recognizes the commitments set forth in the Citywide Privacy Protection Policies and Protocols of the Chief Privacy Officer of the City of New York ("CPO Policies & Protocols"), and is designed to protect and manage information subject to that policy in a consistent and comprehensive manner.

2.0 Authority

2.1 This policy is issued pursuant to the Citywide CSP and the authorizations and authorities cited therein.

3.0 Enforcement

3.1 Each Covered Organization Leader possesses primary responsibility and accountability for adherence to and enforcement of this policy and any related policy and standards within its Covered Organization.

3.2 In accordance with the Citywide CSP Section 6.3, to the extent NYC3 identifies material non-compliance by a Covered Organization with this policy, it shall notify the First Deputy Mayor promptly. The First Deputy Mayor may take such actions as deemed necessary to remedy the non-compliance.

3.3 City employees found to have violated this policy may be subject to disciplinary action, and in certain instances, civil or criminal penalties.

3.4 Any System that does not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Security Officer for the City of New York.

3.5 NYC3 may conduct periodic audits to review the security posture of any System, as well as the information provided during the Information Classification process and the Cybersecurity Risk Assessment process.

4.0 Scope

4.1 Who is Covered?

4.1.1 This policy applies to all Covered Organizations per the Citywide CSP Section 3.1.

(1) Entities working on behalf of or in service to each Covered Organization shall adhere to the requirements set forth in this policy. Each Covered Organization is responsible for their adherence.

4.2 What is Covered?

4.2.1 This policy applies to all City Information that is processed, stored or transmitted on any System owned, maintained or operated by or on behalf of a Covered Organization thereof. Such information is designated as "Information" for purposes of the Citywide CSP.

5.0 Requirements

5.1 Information Handling:

5.1.1 All Information designated as “Restricted” or “Sensitive” shall be handled in accordance with the *Citywide Information Management Standard, (S-ID-RA-02)*.

5.2 Information Storage:

5.2.1 All Information designated as “Restricted” or “Sensitive” shall be stored in accordance with the *Citywide Information Management Standard, (S-ID-RA-02)*.

5.3 Information Labeling:

5.3.1 Information shall be marked appropriately to ensure that users are aware of the sensitivity of the information and how it should be protected and controlled.

5.4 Information Transmission:

5.4.1 Any external transmission of any Information designated as “Restricted” or “Sensitive” shall be encrypted in accordance with the *Citywide Information Management Standard, (S-ID-RA-02)*.

6.0 Roles and Responsibilities

6.1 Covered Organization Leader

6.1.1 Responsible and accountable for the implementation of the Citywide CSP, including this policy.

6.1.2 Responsible for protecting and managing all Information processed, stored or transmitted on their Systems or on Systems of Entities working on behalf of or in service to its Covered Organization.

6.1.3 Responsible for the enforcement of this policy within its Covered Organization.

6.1.4 Responsible for the enforcement of this policy with the Entities working on behalf of or in service to its Covered Organization.

6.2 NYC3

6.2.1 In consultation with DoITT, establish Information Management requirements.

6.2.2 In accordance with the *Citywide Cybersecurity Audit Policy*, audit the Covered Organization protection and management of the Information according to the criteria set forth in this Policy.

6.2.3 Notify the First Deputy Mayor of material non-compliance with this policy by a Covered Organization.

6.3 DoITT

6.3.1 Consult with NYC3 on the Information Management requirements.

6.3.2 Responsible and accountable for the implementation of this policy on Systems it owns, maintains and/or operates.

7.0 Definitions

7.1 Below are several of the defined terms used in this policy. See Citywide Glossary of Defined Terms.

7.1.1 Covered Organization

7.1.2 Covered Organization Leader

7.1.3 Citywide Cybersecurity Program (the "Citywide CSP")

7.1.4 Chief Information Security Officer for the City of New York (the "CISO")

7.1.5 DoITT

7.1.6 First Deputy Mayor

7.1.7 Information

7.1.8 Information Classification

7.1.9 Information Management

7.1.10 NYC3

7.1.11 Restricted Information

7.1.12 Sensitive Information

7.1.13 System(s)

7.2 Current definitions for defined terms can be found in the Citywide CSP Glossary, located on CityShare.

8.0 References

8.1 Citywide Cybersecurity Program, version 1.0.

8.2 National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1 (April 2018).

8.3 NIST Special Publication (SP) 800-30, rev. 1, Guide for Conducting Risk Assessments (Sept. 2012).

8.4 NIST Special Publication (SP) 800-53, rev. 4, Recommended Security Controls for Federal Information Systems (April 2013).

8.5 CIS Top 20 Critical Security Controls, version 7.1, (April 2019).

8.6 NISTIR 7298 Rev. 3 (DRAFT), Glossary of Key Information Security Terms (Sept. 2018)

9.0 Related Citywide Policies and Standards

9.1 Citywide Privacy Protection Policies and Protocols.

9.2 Citywide Information Classification Policy, (P-ID-RA-01).

9.3 Citywide Information Classification Standard, (S-ID-RA-01).

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

9.5 Citywide Cybersecurity Categorization of Information and Systems Policy, (P-ID-RA-03).

9.6 Citywide Cybersecurity Categorization of Information and Systems Standard, (S-ID-RA-03).

9.7 Citywide Inventory Policy, (P-ID-AM-01).