Cyber Command

Topic: Citywide Cybersecurity Program Policies	**No**: P-PR-PT-01
CSP Function: Protect, Detect, Response **CSP Protect Category**: Information Protection Processes and Procedures, Protective Technologies **CSP Detect Category**: Anomalies and Events, Security Continuous Monitoring, Detection Processes **CSP Response Category**: Analysis, Mitigation	**Effective Date:** 10/23/2019
Title: Citywide End-point Security 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	Version 1.1 issued	DOITT	7/28/ 2008
1.2	Updated header with new NYC logo and added this revision history table to the document	DOITT	6/16,/2011
1.3	Updated to reflect the introduction of the Citywide managed anti-virus security cloud, bullet 3. Updated various bullets for greater clarity	DOITT	9/21/2012

1.4	Policy review and minor formatting updates	DOITT	9/9/2014
1.5	Changes Policy to conform to Citywide Cybersecurity Program. Call out NYC3 Managed End-Point Security Program. 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 control requirement to ensure that all Systems owned, maintained or operated by or on behalf of the City of New York ("NYC" or the "City") are protected from malicious software, including, but not limited to Worms, Viruses, Spyware and Malware, and malicious links.

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 Covered Organization System, as well as the information provided during the Information Classification process or 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.

4.1.1.1 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 Covered Organization Systems. A Covered Organization System includes:

4.2.1.1 All Systems owned, maintained or operated by or on behalf of a Covered Organization.

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

4.2.1.3 All Systems that process, access, or transfer City Information.

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

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

5.0 Requirements

5.1 End-point Security Requirements

5.1.1 All Covered Organizations shall enroll all Systems in NYC3 Managed End-Point Security Program as part of its Covered Organization CSP.

5.1.1.1 All Covered Organizations shall deploy NYC3 Managed End-Point Security Agent(s) to all enrolled Systems for which the operating system can support it.

5.1.1.2 All Covered Organizations shall configure all enrolled Systems to the standard secure configuration baseline as defined by the NYC3 Managed End-Point Security Program.

5.1.1.3 All Covered Organizations shall incorporate the NYC3 Managed End-Point Security Agent(s) and the standard secure configuration baseline into their standard image.

5.1.1.4 In accordance with the Citywide Inventory Policy, all Systems participating in the Citywide Managed End-Point Security Program shall be included in the Covered Organization's System Inventory and associated with the relevant end-point security program.

5.1.1.5 All Covered Organizations shall identify and decommission any Systems running operating systems or software that no longer receives security patches or updates.

5.1.2 All Covered Organizations shall timely update any deployed NYC3 Managed End-point Security Agent(s), pursuant to policies, notices, or directives established by NYC3.

5.1.2.1 All Covered Organizations shall assign responsibility for validating version and signature files for stand-alone computers that are not connected to a City-owned Network.

5.1.2.2 Whenever possible, End-point Security updates shall be installed without User intervention.

5.1.2.3 All Covered Organizations shall deploy new end-point policies and configurations for the NYC3 Managed End-point Security Agent within the timeframe specified by NYC3, in accordance with established routine and emergency change management policies.

(A) To the extent that a Covered Organization cannot update the End-point Security Agent within the specified time-frame for release it shall notify NYC3 in accordance with the *End-Point Security Standard*.

5.1.2.4 All Covered Organizations shall deploy a new version of the End-point Security Agent(s) as designated by NYC3 within the timeframe specified by NYC3, in accordance with established routine and emergency change management policies.

(A) To the extent that a Covered Organization cannot update the End-point Security Agent within the specified time-frame for release it shall notify NYC3 in accordance with the *End-Point Security Standard*.

5.1.3 Users shall be prevented from disabling any NYC3 Managed End-point Security Agent(s) installed on City-provided Systems.

5.1.4 Authorized Administrators may temporarily disable or alter containment settings of NYC3 Managed End-point Security Agent(s) for trouble-shooting and/or software installation purposes only with the prior approval of NYC3 and shall immediately re-enable upon completion of trouble-shooting/installation and notify NYC3, in accordance with the End-Point Security Standard.

5.2 Monitoring

5.2.1 In accordance with the *Citywide Vulnerability Management Policy (P-DE-CM-01)*, DOITT and respective Covered Organization CISOs shall scan Networks and Systems for malicious software, including, but not limited to Worms, Viruses, Spyware and Malware.

5.2.2 In accordance with the *Citywide Vulnerability Management Policy (P-DE-CM-01)*, NYC3 may scan Networks and Systems for malicious software, including, but not limited to Worms, Viruses, Spyware and Malware, and malicious links.

5.2.3 The City's Security Operations Center may, in order to preserve the overall security of City Systems, quarantine any City-owned Network or System that exhibits behavior that poses a risk or is infected with unauthorized or malicious software.

5.3 Email Requirements

5.3.1 All electronic mail entering and leaving a City-owned Network (*i.e.*, to or from the Internet) shall be scanned for malicious software, including, but not limited to scanning for Worms, Viruses, Spyware and Malware, and malicious links.

5.3.2 Electronic mail entering or leaving a City-owned Network may be blocked on the basis of detected spam or threats.

5.4 Threat Reporting

5.4.1 Covered Organizations not directly connected to a City-owned Network shall report more than five observations of the same or similar unauthorized or malicious software to the City's Security Operations Center within 24 hours, following the *Citywide Incident Response Policy*.

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 implementation of the controls set forth in this policy within 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 collaboration with DOITT, establish End-point security requirements.

6.2.2 In accordance with the *Citywide Cybersecurity Audit Policy*, audit relevant End User and Systems for compliance with 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 Collaborate with NYC3 on End-point security 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 standard. See Citywide Glossary of Defined Terms.

7.1.1 Application

7.1.2 Authorized Administrator

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

7.1.4 City-owned Network

7.1.5 Citywide

7.1.6 Citywide Cybersecurity Program ("Citywide CSP")

7.1.7 Covered Organization

7.1.8 Covered Organization Leader

7.1.9 DOITT

7.1.10 NYC3 Managed End-point Security Agent

7.1.11 NYC3 Managed End-Point Security Program

7.1.12 First Deputy Mayor

7.1.13 Information Asset

7.1.14 Interface

7.1.15 Malware

7.1.16 Monitoring

7.1.17 Network

7.1.18 NYC3

7.1.19 Outbreak

7.1.20 Spam

7.1.21 Spyware

7.1.22 System

7.1.23 User

7.1.24 Virus

7.1.25 Worm

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) 800-53, rev. 4, Recommended Security Controls for Federal Information Systems.

8.4 CIS Top 20 Critical Security Controls, version 7.1, April 2019.

8.5 NISTIR 7298 Rev. 3 (DRAFT), Glossary of Key Information Security Terms.

9.0 Related Citywide Policies and Standards

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

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

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

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).

9.8 Citywide Vulnerability Management Policy, (P-DE-CM-01).

9.9 Password Policy.

9.10 Multi-Factor Authentication Policy.

9.11 User Responsibilities Policy.