Cyber Command

| | |
|---|---|
| **Topic**: NYC Cybersecurity Program Policies & Standards | **No**: P-DE-CM-01 |
| **CSP Function**: Identify, Detect<br>**CSP Identify Category**: Risk Assessment<br>**CSP Detect Category**: Security Continuous Monitoring | **Effective Date:** 10/23/2019 |
| **Title:** Citywide Vulnerability Management Policy | **Policy Classification:** Non-Restricted |
| | **Issued By:** NYC Cyber Command ("NYC3")<br>**Contact Info**: Policies@cyber.nyc.gov |

**Revision History:**

| Version | Description of Change | Approver | Date |
|---|---|---|---|
| 1.2 | Version 1.2 issued | DOITT | 9/3/2008 |
| 1.3 | Updated header with new NYC logo and added this revision history table to the document | DOITT | 6/16/2011 |
| 1.4 | Policy review and minor formatting updates | DOITT | 9/9/2014 |
| 1.5 | Changes Policy to conform to Citywide Cybersecurity Program.<br>Reformat 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 formal and documented Citywide Vulnerability Management Program (VMP) that defines a standardized method for identifying, assessing, and mitigating vulnerability risk on technology assets across all Covered Organizations per the Citywide CSP Section 3.1.

1.3 This policy establishes a requirement for Covered Organizations to identify Covered Organization technology Assets with vulnerabilities, review vulnerability risk scoring and prioritization provided by NYC3, and mitigate the identified and prioritized vulnerabilities.

# 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 Covered Organization's compliance with the vulnerability management requirements set forth in this policy.

# 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 technology Assets, including Systems and Software, and Environments, which also include cloud environments.

# 5.0 Requirements

5.1 Identify

5.1.1 Covered Organizations shall conduct regular vulnerability scanning to accurately identify vulnerabilities in a timely manner on all their technology Assets.

5.1.2 NYC3 shall provide Covered Organizations assistance to meet the vulnerability scanning identification requirements. Details of these options are outlined in the *Citywide Vulnerability Identification Standard (S-DE-CM-01)*.

5.1.3 Covered Organizations shall conduct regularly-scheduled authenticated scans in accordance with the scanning cadences detailed in the *Citywide Vulnerability Identification Standard (S-DE-CM-01)*.

5.1.4 NYC3 may conduct ad-hoc vulnerability scans.

5.2 Assess

5.2.1 NYC3's Vulnerability Risk Prioritization Program (VRPP) shall assign vulnerabilities, technology Assets, and Asset groups a vulnerability risk score which is categorized and prioritized for mitigation by Covered Organizations.

5.2.1.1 Details of the risk scoring criteria and impacts of prioritization are described in the *Citywide Vulnerability Identification Standard (S-DE-CM-01)*.

5.2.2 Covered Organizations shall review the results of the vulnerability risk scoring and prioritization and act on the prioritization to mitigate vulnerabilities within their technology Assets.

5.3 Mitigate

5.3.1 Each Covered Organization Leader is accountable for mitigating the identified and prioritized vulnerabilities within their technology Assets.

5.3.1.1 For Covered Organizations the mitigation strategy shall rely on the criteria of the three risk factors (asset priority value, vulnerability risk score, and asset's external exposure) as measured by VRPP.

5.3.1.2 The three criteria are factored to derive the Asset Risk Score, which provides the primary means to measure the overall risk posture of asset groups owned or operated by a Covered Organization.

5.3.1.3 The effectiveness of Covered Organization's mitigation strategy shall be measured through the reduction in the Asset Risk and the Asset Group Risk Scores. Asset Risk Score and risk criteria are further defined in the *Citywide Vulnerability Identification Standard (S-DE-CM-01)*.

5.3.2 Mitigation timelines vary based on the Asset Risk Score. The *Citywide Vulnerability Mitigation Standard (S-DE-CM-02)* includes required mitigation timelines for Covered Organizations mitigation and exception handling.

5.3.3 NYC3 may require Covered Organizations to perform expedited mitigation.

5.3.4 NYC3 shall review vulnerability scan results to verify mitigation timelines are met and provide quarterly reports to the Leader of each Covered Organization, Chief Information Security Officer of the City of New York (NYC CISO), and/or the Office of the Mayor (or his or her designee), as detailed in the *Citywide Vulnerability Mitigation Standard (S-DE-CM-02)*.

5.3.5 Covered Organization Leaders shall cooperate with NYC3 to develop an audit program associated with each Covered Organization's Cybersecurity Program (CO CSP).

5.3.6 Audits may be conducted by Covered Organization audit staff, NYC3, or third-parties retained by NYC3.

5.3.7 All audit findings shall be shared with the Covered Organization Leader, NYC CISO, and the First Deputy Mayor (or his or her designee).

# 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 Vulnerability Management requirements.

6.2.2 In accordance with the *Citywide Cybersecurity Audit Policy*, audit relevant Covered Organization processes for compliance with this requirements 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 Collaborate with NYC3 on the Vulnerability 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 the defined terms used in this policy. See Citywide Glossary of Defined Terms.

7.1.1 Asset Vulnerability Risk Score

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

7.1.3 Citywide

7.1.4 Citywide Cybersecurity Program (the "Citywide CSP")

7.1.5 DoITT

7.1.6 Information (or "City Information")

7.1.7 Network

7.1.8 NYC3

7.1.9 System

7.1.10 Technology Asset

7.1.11 Vulnerability

7.1.12 Vulnerability Assessment

7.1.13 Vulnerability Classification

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) Special Publication (SP) 800-60, Vol. I, rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories.

8.3 NIST Special Publication (SP) 800-18; rev. 1, Guide for Developing Security Plans for Federal Information Systems.

8.4 NIST Cybersecurity Framework, version 1.1 (April 2018).

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

8.6 NIST Special Publication (SP) 800-40, rev. 3, Guide to Enterprise Patch Management Technologies.

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

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

# 9.0 Related Citywide Policies and Standards

*9.1 Citywide Vulnerability Identification Standard (S-DE-CM-01)*

*9.2 Citywide Vulnerability Mitigation Standard (S-DE-CM-02*

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

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

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

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

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

*9.8 Citywide Cybersecurity Classification of Information and Systems Policy, (P-ID-RA-03).*

*9.9 Citywide Cybersecurity Classification of Information and Systems Standard, (S-ID-RA-03).*

*9.10 DOITT Citywide Identity Management Security Policy.*

*9.11 Multi-Factor Authentication Standard.*

*9.12 Citywide Privacy Protection Policies and Protocol.*