The City of New York

CITYWIDE INFORMATION SECURITY POLICY

Vulnerability Management Policy

The Policy

All City of New York information systems must be monitored for vulnerabilities to maintain their operational availability, confidentiality, and integrity.

Background

Vulnerability management is a security practice designed to discover and mitigate information technology vulnerabilities that may exist in the Citywide technology infrastructure. Proactively managing vulnerabilities of information systems reduces the potential for exploitation.

Scope

This policy specifically targets City agencies and covers all computing resources directly operationally controlled by the City of New York.

System Inventory

1) All computing resources must be inventoried to determine the types of hardware, operating systems, and software applications that are used within the organization.

2) The computing resource inventory must be periodically reviewed and updated in order to accurately reflect the environment. The inventory must be updated whenever new resources, hardware, operating systems, or software are added to the environment.

Monitor for Vulnerabilities and Threats

3) Agencies must continuously monitor sources of threat and vulnerability information from internal and external security sources.

4) Agencies must perform a timely review of vulnerability information received from reputable sources.

5) Proper analysis must be performed to confirm applicability of identified vulnerabilities in comparison to system inventory.

6) Applicable vulnerabilities must be categorized according to a vulnerability classification. Classification at minimum should consist of urgent, routine, or not applicable.

Remediation and Mitigation of Vulnerabilities

7) Agencies must have a process to remediate vulnerabilities based on significance.

8) Agencies must use automated patch management tools to expedite the distribution of patches to systems.

9) Agencies must maintain a process that develops an action plan to remediate all verified vulnerabilities

Vulnerability Confirmation

10) All agencies with a direct Citynet connection shall participate in DoITT’s automated vulnerability management program and meet the Citywide Vulnerability Management Standard when published.

11) Agencies without a direct Citynet connection must maintain a suitable vulnerability management process.

12) Agencies must verify vulnerability remediation through network and host vulnerability scanning.

Document Revision History

Date	Description
September 3, 2008	**Version 1.2** Issued.
June 16, 2011	**Version 1.3** Updated header with new NYC logo and added this revision history table to the document.
Sept. 9, 2014	**Version 1.4** Policy review and minor formatting updates.