NYC Cyber Command

Topic: Citywide Cybersecurity Program Policies & Standards	**No**: P-02-PR-AC
CSP Function: Protect **CSP Protect Category:** Identity Management, Authentication and Access Control	**Effective Date:** 9/29/2020
Title: Citywide Logon Banner 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
1.0	Initial version	DOITT	7/7/2011
1.1	Changed classification of this policy from sensitive to public	DOITT	4/19/2012
1.2	Policy review and minor formatting updates	DOITT	9/9/2014
1.3	Changes Policy to conform to Citywide Cybersecurity Program (CSP) and reformats document to new NYC Cyber Command Template. Adjusted the scope of the policy to align with the Citywide CSP. Moved the requirements of what the Logon Banner shall cite to the Logon Banner Standard.	NYC3 (Geoff Brown)	9/10/2020

Table of Contents

1.0. Purpose

1.1 The displaying of logon banners prior to a user's authentication onto any System or Network makes users aware of ownership and prohibits unauthorized access. They are an effective security control to support the safeguarding of Systems, Networks, and Information when deployed with other security controls. They educate users and support legal actions on behalf of a Covered Organization by providing reasonable assurance that a user gaining unauthorized access to a System or Network did so knowingly and intentionally.

1.2 The purpose of this policy is to define rules and requirements with regards to the use of logon banners on any City System or Network.

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

2.0. Scope: Who and What are Covered?

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

2.1.1 Entities working on behalf of or in service to each Covered Organization shall adhere to the requirements set forth in this standard. Each Covered Organization is responsible for ensuring adherence by entities that perform work or provide service on their behalf.

2.2 This policy applies to City Systems. This includes:

2.2.1 All Systems owned, leased, licensed, maintained, or operated by or on behalf of a Covered Organization.

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 Information.

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 Information, to fulfill its legal responsibilities, and to protect individuals.

2.3 This policy applies to all production, test, and research development Systems.

2.4 This policy applies to all Networks owned, leased, operated, licensed, or maintained by or on behalf of a Covered Organization.

2.4.1 This includes the City-owned Networks operated and maintained by the Department of Information Technology and Telecommunications.

3.0. Requirements

3.1 Prior to a user's authentication onto any System or Network as defined in Section 2.2, a logon banner shall be displayed.

4.0. Roles and Responsibilities

4.1 Covered Organization Leader

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

4.1.2 Responsible for implementation of the controls set forth in this policy within its Covered Organization.

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

4.2 NYC3

4.2.1 In consultation with DoITT, establish Logon Banner requirements.

4.2.2 In accordance with the Security Audit Policy, audit relevant Covered Organization Networks and Systems for compliance with this policy.

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

4.3 DoITT

4.3.1 Consult with NYC3 on the Logon Banner requirements.

4.3.2 Responsible and accountable for the implementation of this policy on Systems and Networks owned, leased, licensed, maintained, or operated by or on behalf of DOITT.

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 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.

6.2 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.

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

6.4 Any Network or 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.

6.5 NYC3 can conduct periodic audits to review the security posture of any Network or System as well as the information provided during the Information Classification process.

7.0. Definitions

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

7.1.1 Authentication

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

7.1.3 Citywide Cybersecurity Program (CSP)

7.1.4 Covered Organization

7.1.5 Covered Organization System

7.1.6 Covered Organization Leader

7.1.7 DoITT

7.1.8 First Deputy Mayor

7.1.9 IaaS

7.1.10 Logon Banner

7.1.11 Network(s)

7.1.12 NYC3

7.1.13 PaaS

7.1.14 SaaS

7.1.15 System(s)

7.1.16 Third-Party

7.1.17 User(s)

8.0. References

8.1 Citywide Information Security 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.

8.6 NIST Special Publication (SP) 800-50, Building an Information Technology Security Awareness and Training Program (October 2003).

8.7 SANS Institute: Information Security Reading Room, Logon Banners (February 2019).

9.0. Related Citywide Policies and Standards

9.1 Citywide Privacy Protection Policies and Protocols.

9.2 Citywide Logon Banner Standard, (S-01-PR-AC).

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

9.4 NYC3 Inventory Policy, (P-ID-AM-01).

9.5 NYC3 Security Audit Policy.