Cyber Command

P-AS-01

Policy – CityWide Application Security

Policy Effective Date: November 1st, 2018

1 PURPOSE

This document defines the policy for addressing Application Security through appropriate secure coding and configuration practices. All applications must implement adequate security measures to protect the Confidentiality, Integrity, and Availability of data at rest, in use or in motion. This policy is supported by the Application Security Standard. This policy does not conflict, pre-empt, or in any way intervene with the Agency's responsibility to adhere to all appropriate local, state, and federal laws and guidelines pertaining to information security.

2 SCOPE

2.1 This policy applies to all NYC agencies, offices, departments, entities, and personnel, working on behalf of or in service to New York City's municipal government. This policy is consistent with NIST 800-53 controls.

2.2 All applications that pass or store data owned by the City of New York are subject to this policy. All externally accessible public facing applications, internally accessible mission critical applications, vendor customizable Commercial Off-The-Shelf (COTS) or in-house developed applications and cloud based applications are included within the scope of this document.

3 ROLES AND RESPONSIBILITIES

3.1 Agency head is responsible for:

3.1.1 Ensuring the correct and thorough implementation of CityWide cybersecurity policies throughout the entire agency.

3.1.2 Ensuring the completeness and adequacy of all City Agency activities and documentation provided to ensure compliance with CityWide cybersecurity policies throughout the entire agency.

3.1.3 Ensure the development and implementation of adequate controls enforcing the Application Security Policy for the agency.

3.1.4 Ensuring CityWide policies are periodically reviewed and controls are put in place to reflect changes in requirements.

3.1.5 Ensure all personnel understand their responsibilities with respect to planning and implementing application security.

3.1.6 Ensure users are appropriately trained and educated on the Application Security Policy, Standards and Procedures.

4 POLICY

4.1 This policy requires NYC agencies to establish management responsibilities and procedures to ensure application security by design and implementation.

4.2 **Application Criticality Classification** - All applications must be classified based on the level of criticality in accordance with the Data Protection Policy and the System (Application) Classification Questionnaire.

4.3 **Data Security** - Protecting data's confidentiality, integrity and availability is a principle that must be maintained at all times. Proper data protection mechanisms (including, but not limited to, encryption) must be implemented to protect data at rest, in use or in motion (C.f. CityWide Encryption Policy).

4.4 **Access Control** - All access to City of New York systems must be authorized and based on individual identification and authentication. All applications must comply with the CityWide Identity Management Policy, Password Policy and External Identity Management and Password Policy

4.5 **Infrastructure Security** - Application hosting solutions must comply with the City's security policies and standards and have a Service Level Agreement defined with the infrastructure provider. The infrastructure environment must be scanned on a periodic basis (C.f. Vulnerability Management Policy).

4.6 **Application Environment** - Application environments must have security mechanisms in place. Development activities may only be conducted in a non-production environment. Separation of duties must be implemented to protect the production environment from unauthorized modification. Change control procedures must be defined to ensure that only authorized changes can be released to production.

4.7 **Security Assessment and Releases to Production** - Modifications of the application must go through a change release process that includes an appropriate security assessment. Application changes deployed in a production environment must comply with the City's security policies and must have the CityWide Chief Information Security Officer (CCISO) acknowledge the completion of the security assessment. Each release must also have a defined roll-back plan

4.7.1 **Security Assessment**: Full, quick, and targeted assessment levels must be established to test for vulnerabilities.

4.7.2 **Releases to Production**: Releases to a production environment are approved based on the vulnerabilities found during the security assessment. All security issues that are discovered during assessments or identified by the City's Software Security Assurance Tool must be mitigated based upon their risk levels.

4.8 **Business Continuity** - Each application must have a defined Business Continuity Plan and a Disaster Recovery plan. These plans ensure that back-up and recovery solutions are implemented in the case of a disruption to the application's service.

4.9 **Application End of Life** - Decommissioning an application requires the same security precautions as maintaining it in production. Regulatory requirements regarding data retention and destruction must be considered as the application is decommissioned

4.10 **Building Applications** - Software Security Assurance (SSA) - The SSA process ensures that software is designed to operate at a level of security consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls and protects.

The objective is to provide guidance and support to project and development teams in delivering secure applications to support the City's business while expediting the security assessment and testing process required to validate new application releases are free of vulnerabilities that would put the production environment at risk.

The CityWide Chief Information Security Officer has established a tool available at https://appsec.cityofnewyork.us to identify security requirements for in-house developed and modified COTS applications based on their architecture, back-end technologies, and applicable regulations.

5 NON-COMPLIANCE

5.1 City employees found to have violated this policy may be subject to disciplinary action.

5.2 Any software application 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.

5.3 NYC Cyber Command can conduct periodic audits to review the security posture of any Information System, as well as the information provided during the Application Security Assurance Process.

5.4 Policy Exceptions

5.4.1 Exceptions require a documented business justification. Exceptions are subject to the approval of the CityWide CISO or designee.

5.4.2 Requests for exceptions of high risk issues may only be made by an agency's Information Security Officer (ISO) and Commissioner.

5.4.3 Requests for exceptions of medium and low risk issues may only be made by an agency's Information Security Officer (ISO) or application's business owner

6 AUTHORITY

The New York City Cyber Command ("NYC3"), in collaboration with the New York City Department of Information Technology and Telecommunications ("DoITT"), issues this Application Security Policy pursuant to Mayoral Executive Order 28 of 2017. This policy applies to any technology system owned, maintained, and/or operated by any agency of the City of New York ("City agency") and to any agency that connects a device or network to any such system ("Non-City Agency"). The requirements contained here are binding on all City and Non-City Agency heads.

7 REFERENCES

7.1.1 P-RA-02: Security Categorization of Information Types and Information Systems – September 2018

7.1.2 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"

7.1.3 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

7.1.4 Payment Card Industry Data Security Standard (PCI DSS) v2.0, PCI Security Standards Council, October 2010.

7.1.5 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2010.

GLOSSARY

An application	An application, also referred to as an application program or application software, is a computer, mobile or IoT platform software package that performs a specific function directly for an end user or, in some cases, for another application (also referred to as a service application).

Production Environment	Any on-premises or cloud based production environment managed by a city agency