



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

APPLICATION DEVELOPMENT SECURITY

THE POLICY

ALL SYSTEMS AND APPLICATIONS THAT PROCESS OR STORE CITY OF NEW YORK INFORMATION SHALL ADDRESS INFORMATION SECURITY REQUIREMENTS DURING ALL PHASES OF THE DEVELOPMENT CYCLE.

SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATIONS

- 1) An assessment will be conducted by the business and/or system owner to identify the type of information that will be stored, processed or transmitted by the system.
- 2) Stringency of system security requirements will be defined in accordance to the value of the data contained in the system.
 - a. Systems that contain personal identifiable information (PII) or personal health information (PHI) must comply with all applicable regulatory statutes.
- 3) A comprehensive security requirements analysis will be performed for all new systems and for significant upgrades to existing systems. The security analysis will assess compliance to the Citywide Information Security Policies.
- 4) System security requirements and specifications must be compliant with industry best practice standards for technologies and system configuration and Citywide Information Security Standards where applicable.
- 5) System security requirements and specifications must ensure interoperability with all information sources and services with which it must interface.
- 6) System security requirements and specifications must ensure integration with existing security services where applicable.

SECURITY VERIFICATION

- 7) All new systems must be tested in a separate environment for stability and to identify any unanticipated interactions with existing systems before they are moved to the production environment.
- 8) All new systems must be tested for security integrity and functional verification prior to production release.
- 9) Any new applications that will connect to Citynet must be approved by the Citywide Chief Information Security Officer (CISO) to ensure that there will be no negative impact to Citynet.
- 10) The agency CISO (or equivalent position) must make final approval on all application security which has an agency level impact.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

DEVELOPMENT & TESTING

- 11) The production environment will not be used for development or testing activities.
- 12) All security functionality will be operational during formal acceptance and operational testing.
- 13) Prior to production release of any new application, testing will be done to ensure the new application will not adversely affect any existing systems.
- 14) Newly developed applications and major upgraded applications will be approved for use at the agency by the Chief Information Officer (CIO, or equivalent position) prior to migration to the production environment.

BUSINESS CONTINUITY

- 15) Each application must have a defined back out plan in the unlikely event that its migration to the production environment causes service degradation.
- 16) Each new application must create a business continuity and disaster recovery program in accordance with the business significance of the application.