Application Development Security Policy

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) All externally accessible, public facing applications and internally accessible, multi-agency applications developed to support City of New York business must be approved by the Citywide Chief Information Security Officer (CISO) through the Citywide Security Accreditation Process.
10) The agency CISO (or equivalent position) must make final approval on all application security which has an agency level impact.

Development and 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 must be done and established change control processes followed 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.

Other Security Requirements

15) Web services and distributed components of City applications which handle data classified as PRIVATE or higher shall require client authentication.

16) All applications subject to spam or forms based denial of service (DOS) attacks must employ CAPTCHA or equivalent technology.

17) A source code repository with check-in and check-out capabilities is required for all City-developed applications.

18) PRIVATE or CONFIDENTIAL data may not be copied from any production environment to any lower region or non-production environment unless the data has been masked. Alternatively, PRIVATE or CONFIDENTIAL data may be copied to a non-production environment provided the environment employs full production controls.

Business Continuity

19) Each application must have a defined back out plan in the unlikely event that its migration to the production environment causes service degradation.

Document Revision History

Date	Description
June 16, 2011	**Version 1.3** Updated header with new NYC logo and added this revision history table to the document.
October 18, 2012	**Version 1.4** Added the following text: **Other Security Requirements** Web services and distributed components of City applications which hand data classified as PRIVATE or higher shall require client authentication. All applications subject to spam or forms based denial of service (DOS) attacks must employ CAPTCHA or equivalent technology. A source code repository with check-in and check-out capabilities is required for all City-developed applications. PRIVATE or CONFIDENTIAL data may not be copied from any productior environment to any lower region or non-production environment unless the data has been masked. Alternatively, PRIVATE or CONFIDENTIAL data may be copied to a non-production environment provided the environment employs full production controls. Deleted the following: Each new application must create a business continuity and disaster recovery program in accordance with the business significance of the application.