5. **Application Development**

City of Chicago ("City") staff and contract application developers must use a standardized development framework which requires specific information security steps, to ensure the protection of sensitive information, application availability, and data integrity.

This policy reviews the following areas:

5.1 Security in Development and Support Processes
5.1.1 Separation of Development and Production Environments
5.1.2 Segregation of Duties
5.1.3 Information Leakage
5.1.4 Outsourced Software Development
5.1.5 Technical Review of Applications after Changes

5.2 Secure Coding Standards
5.2.1 Secure Coding Requirements
5.2.2 Input Data Validation
5.2.3 Developer Training

5.3 Security of System Files
5.3.1 Control of Operational Software
5.3.2 Protection of Live Data in Test Environments

5.4 Revision History
5.1 Security in Development and Support Processes

A system development lifecycle methodology, in accordance with current industry best practices and standards for secure application development, must be followed. Clear segregation of duties must be established between release managers, testers, and developers in order to effectively manage viewing, changing, and migration of source code. Additionally, a technical review must be performed after each software change to ensure security standards are met.

5.1.1 Separation of Development and Production Environments

Appropriate requirements and controls must be in place requiring the physical separation of development, test and production environments.

a. Technical Operations and Enterprise Network Architecture must ensure that the production, test, and development environments are physically and/or logically separated.
   ISO: 10.1.4, PCI: 6.3.2

b. Technical Operations and Enterprise Network Architecture must ensure that test environments emulate the production environment as closely as possible, including the use of a common operating system, database, web application server, and similar hardware to the degree possible.
   ISO: 10.1.4

c. Technical Operations and Enterprise Network Architecture must ensure that only authorized release managers and system administrators have access to the production environment where the production executable code for an application resides. Application developers may have read-only access to production log and configuration files as deemed necessary.
   HIPAA: 164.310(a)(1)(iii), ISO: 10.1.4

5.1.2 Segregation of Duties

Segregation of duties controls must be in place to manage the ability to view, change, and to migrate source code. Developers, release managers, and testers must specifically be controlled in the actions they can take in the development, test, and production environments.

a. Application Development must ensure that specific segregation of duties controls are in place and that distinct, separate roles exist for developers, release managers, and testers.
   PCI: 6.3.2

b. Application Development must ensure that developers, release managers, and testers are restricted in the activities they can perform, as defined in the table below.
   PCI: 6.3.2
c. Separation of duties must exist between personnel assigned to the development/test environments and those assigned to the production environment.

PCI: 6.3.3

<table>
<thead>
<tr>
<th>Role</th>
<th>Development</th>
<th>Test</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developer</td>
<td>V, C</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Release Manager</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Tester</td>
<td></td>
<td>V</td>
<td>V</td>
</tr>
</tbody>
</table>

(V)iew: This action allows for the viewing of source code within the environment

(C)hange: This action allows for the changing of source code within the environment

(M)igrate: This action allows for the migration of code between environments

d. **Application Development** and the **Information Security Office** must ensure that directories or repositories containing application source code are secured from unauthorized access.

HIPAA: 164.310(a)(1)(iii), ISO: 12.4.3

e. **Application Development** must ensure that access controls are developed to prevent unauthorized parties from gaining access to source code in an uncontrolled manner. This includes restricted access for developers to production systems and monitoring of access by developers to production systems during maintenance or support activities.

HIPAA: 164.310(a)(1)(iii), ISO: 12.4.3

f. Source code must not be stored on production systems when possible.

ISO: 12.4.3

g. **Application Development** must ensure that access levels restrict developers from making changes to the code maintained in the test environment during acceptance testing. When appropriate, a change control software tool must be utilized to ensure that programmers are adequately restricted from accessing production environments and testing environments.

HIPAA: 164.310(a)(1)(iii), ISO: 12.4.3

h. **Application Development** must ensure that all changes to code are logged in a central version control solution. To the extent possible, this solution should also log all access to source code files.

ISO: 12.4.3

i. **Application Development** must ensure that access and modification access is properly assigned. During acceptance and system testing, logical access restrictions must ensure that developers have no update access and that the code being tested cannot be modified without the consent of the user. The developer must make appropriate modifications in the development environment and submit it to the release engineer for retesting.

HIPAA: 164.310(a)(1)(iii), ISO: 12.5.1
5.1.3 Information Leakage

Controls must be implemented to prevent information leakage at system runtime.

a. Application Development must ensure that system information provided through error messages does not provide any information about an application's architecture or the City network.
   
   HIPAA: 164.310(a)(1)(iii), ISO: 12.5.4, PCI: 6.5.6

5.1.4 Outsourced Software Development

All outsourced development must be reviewed and approved by appropriate City personnel. In addition, all contracts for outsourced development must include the necessary provisions to ensure secure coding.

a. All contracts for outsourced development must be reviewed by the Department of Law and Application Development.
   
   ISO: 12.5.5

b. All code, software, or infrastructure provided by an outsourced development contractor must be reviewed and accepted in writing by Application Development in conjunction with the Information Security Office.
   
   ISO: 12.5.5

c. The Department of Law must ensure that all outsourced software development contracts provide protections for the City including the following:
   
   - Licensing arrangements, code ownership, and intellectual property rights
   - Service level agreements, including quality assurance and control of delivered software
   - “Right to audit” contractor’s processes, infrastructure, development methodologies, security or any other control area deemed necessary by Internal Audit
   - Acceptance requirements
   
   ISO: 12.5.5

d. Application Development is responsible for monitoring all activity performed by software development firms engaged by the City.
   
   ISO: 12.5.5

e. Application Development or any Department or Business Unit seeking to contract for outsourced software development must notify the Department of Innovation and Technology prior to the release of any requests for proposal or information.
   
   ISO: 12.5.5
5.1.5 Technical Review of Applications after Changes

All software releases and updates/patches to production systems must to be tested for functionality and security.

a. After changes (e.g., patches, upgrades, or new versions), Application Development must ensure that applications and support processes are reviewed and tested as deemed necessary. These processes include but are not limited to the following

- Application control and integrity procedures
- Support and development plans for operating system changes
- Proper notification of changes to user community
- Updates to any applicable business continuity plans and/or recovery processes

HIPAA: 164.312(c)(1), ISO:12.5.2

b. Application Development must ensure that all new or modified software, including the application of patches, is adequately tested, approved, and consistent with change and management standards before being deployed to the City's production environment. Such testing must include validation of input into the application, proper error handling, proper use of Role Based Access Controls (RBAC), secure cryptographic storage, and secure cryptographic communications as required for specific data and within the cardholder environment.

ISO: 12.5.1, PCI: 6.3.1

c. Code changes must be reviewed by individuals (other than the originating code author) educated in the execution of code review techniques and secure coding practices, or by an automated code review tool approved by Application Development. Based on the code review results, appropriate corrections must be made, and the code review results must be reviewed and approved by management prior to release into production.

PCI: 6.5, 6.3.7

d. Application Development must ensure that all significant modifications, major enhancements, and new systems undergo system testing prior to installation in production. System stress testing, volume testing, and parallel testing should be performed as appropriate. System testing must be conducted in a separate, independently-controlled environment.

ISO: 12.5.1

e. Application Development must ensure that all significant modifications, major enhancements, and new systems undergo acceptance testing by the appropriate Application Owners prior to installation in production. The user acceptance plan must include tests of all major functions, processes, and interfacing systems, as deemed necessary.

ISO: 12.5.1
5.2 Secure Coding Standards

Developers must be trained in secure coding techniques such as input validation and restricted error reporting.

5.2.1 Secure Coding Requirements

A secure coding standard must be utilized as part of the software development methodology.

a. All web-based applications must be developed based on a current version of the OWASP secure code guidelines, and must account for the following:

- Cross-site scripting (XSS) (validate all parameters before inclusion)
- Injection flaws, particularly SQL injection (validate input to verify user data, cannot modify meaning of commands and queries)
- Malicious file execution (validate input to verify application does not accept filenames or files from users)
- Insecure direct object references (do not expose internal object references to users)
- Cross-site request forgery (CSRF)
- Information leakage and improper error handling (do not leak information via error messages or other means)
- Broken authentication and session management (properly authenticate users and protect account credentials and session tokens)
- Insecure cryptographic storage (prevent cryptographic flaws)
- Insecure communications (properly encrypt all authenticated and sensitive communications)
- Failure to restrict URL access (consistency enforced access control in the presentation layer and business logic for all URLs)

PCI: 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10

5.2.2 Input Data Validation

Data entered into City application systems must be validated where possible to ensure information quality and mitigate the impacts of web-based attacks.

a. Application Development must implement data checks within information systems and applications to validate business transactions, standing/master data or parameter tables. Dual input checks, such as boundary checking or limiting fields to specific ranges of input data, must be used on critical inputs for systems when applicable. Checks may include:

- Out-of-range validation checks
- Invalid characters in fields
- Mandatory field definition

HIPAA: 164.312(c)(2), ISO: 12.2.1, PCI: 6.5
b. **Application Development** must ensure that all data input fields properly validate the input in order to minimize the threat of cross site scripting and SQL injection.
   
   HIPAA: 164.312(c)(1), ISO: 12.2.1, PCI: 6.3.1.1

c. **Application Development** must ensure that data being entered into City application systems is validated where possible to increase information quality.
   
   HIPAA: 164.312(c)(2), ISO: 12.2.1

d. An application firewall must be configured and placed in front of all externally facing web applications containing private data to detect and prevent external web-based attacks. **Application Development** must be involved in the configuration of the web application firewalls in order to ensure that application-specific requirements are properly accounted for.
   
   PCI: 6.6

### 5.2.3 Developer Training

All City staff and contractor application developers must be properly trained in secure coding standards.

a. The City must ensure its developers are adequately trained in secure coding techniques, based on best practice guidance.

   PCI: 6.5
5.3 Security of System Files

Operational systems must be configured according to the standards set forth in this policy prior to going into a production environment to ensure the security of the files contained within.

5.3.1 Control of Operational Software

All operational software must be an authorized version supported by the vendor, where applicable, and configured securely.

a. Application Development must ensure that operational systems only hold/store approved code. Development code or compilers must not be stored on production systems.
   HIPAA: 164.310(a)(1)(iii), ISO: 10.1.4, 12.4.1

b. Application Development must ensure that vendor-supplied software is maintained at a version supported by the vendor.
   ISO: 12.4.1

c. An audit log of all program updates must be maintained and a library of previous source code versions must be retained.
   HIPAA: 164.310(a)(1)(iii), ISO: 12.4.1

d. Application Development is responsible for archiving old versions of software along with configurations, parameters, procedures and other supporting documentation, as deemed appropriate.
   ISO: 12.4.1

e. Application Development must ensure that updates to operational software, applications and program libraries are performed by designated, trained personnel.
   HIPAA: 164.308(a)(1), ISO: 12.4.1

f. Application Development must ensure that all vendor-supplied default passwords are changed prior to the system being placed in a production environment.
   HIPAA: 164.308(a)(5)(D), ISO: 12.4.1, PCI: 2.1

g. Application Development must ensure that system default settings are reviewed prior to installation to determine potential security holes. Settings that could potentially compromise security must be changed prior to the system being placed into a production environment.
   HIPAA: 164.308(a)(1), ISO: 12.4.1, PCI: 2.1
5.3.2 Protection of Live Data in Test Environments

All data classified as private or higher used in any non-production environment must be altered or obfuscated.

a. Any unaltered production data used for test purposes in nonproduction environments must be approved by Information Owners and the Information Security Office. In the case where production data contains private data elements, the Department of Law must also provide written approval to use or copy production data for test purposes.
   HIPAA: 164.310(a)(1)(iii), ISO: 12.4.2

b. Production data consisting of payment card data must not be used for testing or development.
   PCI: 6.3.4

c. Application developers must ensure that test data, test accounts, custom application accounts, user IDs and/or passwords are removed before a system is implemented into production.
   PCI: 6.3.5, 6.3.6

d. Where production data is copied to a test system, Application Development must ensure that the data is subject to a similar level of control as the production version including all legal, regulatory, or security requirements. The controls must include:
   - Similar authorization methods and procedures for access to the data or test systems
   - Defined plan for deletion of data after testing has been completed
   - Audit log of activity and personnel accessing system and data
   - Similar access controls to production to ensure confidentiality of data is maintained
   HIPAA: 164.308(a)(4)(B), ISO: 12.4.2
5.4 Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/15/2013</td>
<td>0.5</td>
<td>Initial Draft</td>
<td>ISO</td>
</tr>
<tr>
<td>07/26/2013</td>
<td>1.0</td>
<td>Approved as Release Candidate v1</td>
<td>CISO</td>
</tr>
<tr>
<td>12/30/2013</td>
<td>2.0</td>
<td>Approved as Release Candidate v2</td>
<td>CISO</td>
</tr>
</tbody>
</table>