HAMPTON VA

No. IT– 029	Policy Name: Revenue Systems Applications Security Procedure
Effective Date: 7-1-2011 Last Revised Date: 7-4-2014	Citywide Policy _ IT Policy _ IT Procedure X
Approved By: IT Director	

Revenue Systems Applications Security Procedure

Overview

Implementing security policies and best practices, improving user security awareness, and early detection and mitigation of security incidents are some of the actions taken to reduce the risk of security incidents. Security should be an integral part of new systems. When functional requirements are designed, security requirements should be formulated corresponding to the sensitivity and availability of data to be handled by the system.

2. Purpose

The purpose of the Revenue Systems Applications Security Procedure is to describe the requirements for developing and/or implementing software for the offices of the City of Hampton Commissioner of Revenue and Treasurer. This procedure is established in accordance with and as a supplement to Information Technology Security Policy # 09-005.

3. Applications Security Procedure

3.1 The Revenue Systems Team is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for the offices of the City of Hampton Commissioner of Revenue and Treasurer. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical City of Hampton information.

3.2 All production systems must have designated Owners and Custodians for the critical information they process. IT must perform periodic risk assessments of production systems to determine whether the controls employed are adequate.

3.3 All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these Users. A designated access control administrator (who is not a regular User on the system in question) must be assigned for all production systems.

3.4 Where resources permit, there will be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, the following applies:

3.4.1 The application deployment process will include two staff members as follows

3.4.1.1 A staff member that develops software code should not also deploy the code to production;

3.4.1.2 A staff member that did not develop the code should deploy code to production.

3.4.2 In instances where the separation of duties might not be viable for the City of Hampton

3.4.2.1 Emergencies - The Solutions Development Coordinator overseeing the Commissioner of Revenue and Treasurer's system will sign off and review code before it is deployed to production.

3.4.2.2 When skill sets required to separate code development and production are not available with limited city resources - Identify specific modules or applications where this is applicable and invoke item 3.4.2.1 of this procedure as an alternative.

3.5 All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

3.6 Violations of this procedure must be reported to the IT Director or IT Security Manager