Administrative Procedures for Board Policy 05.51 Information Security & Privacy Program Set #4

05.51 AP.121 Technology Development and Acquisition (TDA)

05.51 AP.122 Cryptographic Protections (CRY)

Technology Development and Acquisition (TDA)

SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONAL ENVIRONMENTS

Procedure/Control Activity: Manager Digital Privacy and Cybersecurity, in conjunction with Specialist Enterprise Architects, Assistant Director Infrastructure Services, and Administrator Cybersecurity:

(1) Implements appropriate administrative means to ensure:

a. Asset custodians maintain and manage baseline configurations for development and test environments separately from its production baseline configurations;

b. Production and non-production environments are separated to prevent unauthorized access or changes to information assets; and

c. That developers are prevented from having unmonitored access to production environments.

(2) On at least an annual basis, during the fourth (4th) quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:

a. Distributes copies of the change to key Information, Integration, and Innovation (IT3) personnel; and

b. Communicates the changes and updates to key District personnel.

(3) If necessary, requests corrective action to address identified deficiencies.

Cryptographic Protections (CRY)

TRANSMISSION CONFIDENTIALITY

Procedure/Control Activity: Specialist Enterprise Architect, in conjunction with Assistant Director Infrastructure Services, Associate Systems Engineer, and Manager Digital Privacy and Cybersecurity:

(1) Uses vendor-recommended settings and industry-recognized secure practices to prevent the unauthorized disclosure of information during transmission, through ensuring systems transmitting sensitive information by:

   a. Accepting only trusted keys and certificates;

   b. Using strong cryptography and security protocols – Transport Layer Security (TLS), Internet Protocol Security (IPSEC), and Secure Shell (SSH) – to safeguard sensitive data during transmission over public or private networks;

      i. Examples of public networks include, but are not limited to:

         1. The Internet

         2. Wireless technologies

      ii. Examples of private networks include, but are not limited to:

         1. Local Area Networks (LAN)

         2. Virtual Private Network (VPN)

   c. Verifying that the proper encryption strength is implemented for the encryption methodology in use, based on documented vendor recommendations and industry-recognized secure practices; and

   d. Verifying that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. For TLS implementations:

      i. Verify that Hypertext Transfer Protocol – Secure (HTTPS) appears as a part of the browser Universal Record Locator (URL); and

      ii. Verify that no sensitive data is displayed when HTTPS does not appear in the URL.

(2) On at least an annual basis, during the fourth (4th) quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:

   a. Distributes copies of the change to key Information, Integration, and Innovation (IT3) personnel; and

   b. Communicates the changes and updates to key District personnel.

If necessary, requests corrective action to address identified deficiencies

Cryptographic Protections (CRY)

TRANSMISSION INTEGRITY

Procedure/Control Activity: Associate Enterprise Architect, in conjunction with systems administrators, Associate Systems Engineers, Administrator Cyber Security and Assistant Director Infrastructure Services:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure cryptographic mechanisms prevent unauthorized modification or corruption of information during transmission, including:

a. Secure Shell (SSH)

b. Hypertext Transfer Protocol – Secure (HTTPS)

c. Transport Layer Security (TLS)

d. Advanced Encryption Standard (AES).

(2) On at least an annual basis, during the fourth (4th) quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:

a. Distributes copies of the change to key IT3 personnel; and

b. Communicates the changes and updates to key District personnel.

(3) If necessary, requests corrective action to address identified deficiencies.