Administrative Procedures for Board Policy 05.51 Information Security & Privacy Program Set #3

Change Management

CONFIGURATION CHANGE CONTROL

Procedure/Control Activity: System Administrator, Assistant Director Infrastructure Services, Manager Digital Privacy and Cybersecurity:

(1) Follow published District change control processes in an ITIL Compliant ticketing system for all changes to system components.

(2) Review change requests in a Change Control Board (CAB) that meets on a routine basis.

(3) Utilizes separate environments for development/testing/staging and production.

(4) Remove test data and accounts before production systems become active/goes into production.

(5) Implement security patches and software modifications, which includes, but is not limited to, the following:

a. Documentation of impact;

b. Documented change approval by authorized parties on the CAB; and

c. Functionality testing to verify that the change does not adversely impact the security of the system.

(6) Develop back-out procedures.

(7) On at least an annual basis, during the third (3rd) quarter of the calendar year, review the process for non-conforming instances. As needed, revise processes to address necessary changes and evolving conditions. Whenever the process is updated:

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

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

(8) If necessary, request corrective action to address identified deficiencies.

(9) If necessary, validate corrective action occurred to appropriately remediate deficiencies.

Third Party Management (TPM)

THIRD PARTY MANAGEMENT

Management Intent: The purpose of the Third-Party Management (TPM) policy is to ensure that risk associated with third-parties are minimized or avoided.

Procedure/Control Activity: Manager Digital Privacy and Cybersecurity, in conjunction with Assistant Director Infrastructure Services, Systems Analysts, and the Chief Information Officer (CIO):

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are enough for managing third-party service providers' compliance with cybersecurity, privacy and service delivery requirements included in third-party contracts by:

a. Requiring data/process owners maintain and implement procedures to manage service providers that include:

i. Maintaining a list of service providers;

ii. Maintaining written agreements that include acknowledgments that the service providers are responsible for the security of sensitive data the service providers possess or otherwise store, process or transmit on behalf of the District , or to the extent that they could impact the security of the District;

iii. Monitoring and ensuring there is an established process for engaging service providers, including proper due diligence prior to engagement;

iv. Maintaining a program to monitor service providers' compliance status at least annually; and

v. Maintaining information about which requirements are managed by each service provider, and which are managed by the District; and

b. Utilizing the process of due diligence, including, but not limited to:

i. Direct observations;

ii. Reviews of policies and procedures; and

iii. Reviews of supporting documentation.

(2) On at least an annual basis, at least ninety (90) days prior to contract expiration, 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:

a. Requests corrective action to address identified deficiencies;

Third Party Management (TPM)

b. Validates corrective action occurred to appropriately remediate deficiencies;
c. Documents the results of corrective action and notes findings; and
d. Requests additional corrective action to address unremediated deficiencies.

Configuration Management

SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS

Procedure/Control Activity: Administrator Cybersecurity, in conjunction with the Infrastructure Services and Systems Analysts:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure baseline system hardening configuration for all District-owned or managed assets comply with applicable legal, statutory, and regulatory compliance obligations.

(2) Where technically feasible, technology platforms align with industry-recommended hardening recommendations, including but not limited to:

a. Center for Internet Security (CIS) benchmarks;

b. Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs); or

c. Original Equipment Manufacturer (OEM) security configuration guides.

(3) Ensures that system hardening includes, but is not limited to:

a. Technology platforms that include, but are not limited to:

i. Server-Class Systems;

ii. Workstation-Class Systems;

iii. Network Devices;

iv. Mobile Devices; and

v. Databases

b. Enforcing least functionality, which includes but is not limited to:

i. Allowing only necessary and secure services, protocols, and daemons;

ii. Removing all unnecessary functionality, which includes but is not limited to:

1. Scripts;

2. Drivers;

3. Features;

4. Subsystems;

5. File systems; and

6. Unnecessary web servers.

c. Configuring and documenting only the necessary ports, protocols, and services to meet business needs;

d. Implementing security features for any required services and protocols that are insecure, which includes but is not limited to using secured technologies to protect insecure services;

e. Installing and configuring appropriate technical controls, such as:

i. Antimalware;

Configuration Management

ii. Software firewall;
iii. Event logging; and
iv. File Integrity Monitoring (FIM), as required; and

SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS

f. As applicable, implementing only one (1) primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers, and DNS should be implemented on separate servers).

(4) Documents and validates security parameters are configured to prevent misuse.

(5) Authorizes deviations from standard baseline configurations in accordance with District change management processes, prior to deployment, provisioning, or use.

(6) Validates and refreshes configurations on a regular basis to update their security configuration considering recent vulnerabilities and attack vectors. Unless a technical or business reason exists, standardized images are used to represent hardened versions of the underlying operating system and the applications installed on the system.

(7) On at least an annual basis, during the third (3rd) 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) stakeholders; and

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

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

Capacity and Performance Planning

ADEQUATE CAPACITY TO ENSURE AVAILABILITY IS MAINTAINED

Procedure/Control Activity: Assistant Director Infrastructure Services, in conjunction with Manager Digital Privacy and Cybersecurity and Systems Analysts:

(1) Measures the current availability, quality and adequacy of resources to deliver the required system performance to meet existing Service Level Agreements (SLAs).

(2) Creates projections of future capacity requirements to mitigate the risk of system overload.

(3) Educates stakeholders on requirements to allocate sufficient processing and storage capacity to reduce the likelihood of exceeding capacity that could negatively impact SLAs.

(4) On at least an annual basis, during the third (3rd) 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.

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