Administrative Procedures for Board Policy 05.51 Information Security & Privacy Program

Human Resources Security

HUMAN RESOURCES SECURITY MANAGEMENT

Procedure/Control Activity: The Human Resources Division (HR), in conjunction with Manager Digital Privacy and Cybersecurity, Assistant Director Infrastructure Services:

(1) Implements appropriate administrative and technical means to ensure HR processes are sufficient to address cybersecurity considerations in human resources practices (e.g., personnel screening, position changes, deprovisioning, etc.).

(2) 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 stakeholders; and
b. Communicates the changes and updates to HR, Assistant Director Infrastructure Services.

Project and Resource Management

ALLOCATION OF RESOURCES

Procedure/Control Activity: Information Technology Project Manager, Director Internal Audit, Assistant Director Infrastructure Services, Manager Digital Privacy and Cybersecurity, and Chief Information Officer:

(1) On a monthly basis, reviews the allocation of resources for cybersecurity and privacy projects to provide oversight for the cybersecurity-related aspects of the planning, support and tool selection process. The process:

   a. Includes cybersecurity requirements in business process planning; and
   b. Allocates resources required to protect its systems and data, as part of its capital planning process.

(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 senior Information, Integration, and Innovation Management; and
   b. Communicates the changes and updates to stakeholders and staff.

Maintenance

CONTROLLED MAINTENANCE

Procedure/Control Activity: Infrastructure Services management, in conjunction with asset owners:

(1) Conducts maintenance in a timely manner to minimize downtime and business disruption.

(2) Schedules, performs, documents, and reviews records of maintenance and repairs on systems in accordance with manufacturer or vendor specifications and company requirements.

(3) Controls all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.

(4) Keeps maintenance records for information systems that include:

a. Date and time of maintenance;
b. Name of the individual performing the maintenance;
c. Name of escort, if necessary;
d. A description of the maintenance performed.; and
e. A list of equipment removed or replaced (including asset tag numbers, if applicable).

(5) Requires explicit management approval for the removal of the systems or system components from District facilities for off-site maintenance or repairs.

(6) Sanitizes equipment to remove all information from associated media prior to removal from District facilities for off-site maintenance or repairs.

(7) Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

(8) Obtains maintenance support and spare parts for critical systems and key information technology components within defined Service Level Agreements (SLAs).

(9) On at least an annual basis, during the second (2nd) 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 Information, Integration, and Innovation (IT3) personnel; and
b. Communicates the changes and updates to key district stakeholders.

NON-LOCAL MAINTENANCE

Procedure/Control Activity: Assistant Director Infrastructures Services and the system administrator, in conjunction with asset owner:

(1) Authorizes, monitors, and controls non-local maintenance and diagnostic activities.

(2) Allows the use of non-local maintenance and diagnostic tools only in accordance with District policy and standards.

(3) Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions.

(4) Terminates all sessions and network connections when non-local maintenance is completed.

(5) On at least an annual basis, during the second (2nd) 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 stakeholders.

Threat Management

THREAT AWARENESS

Procedure/Control Activity: Manager Digital Privacy and Cybersecurity, in conjunction with Administrator Cybersecurity, Assistant Director Infrastructure Services, and Information, Integration, and Innovation (IT3) leadership:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for managing a formal threat awareness program that:

a. Identifies the District's place in critical infrastructure and its industry sector; and Communicates this level of importance to all users so that they can be aware of sector-specific threats.

(2) Treats threat information-sharing as:

a. Bilateral (e.g., government-commercial cooperatives, commercial-commercial cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia); and

b. Highly sensitive, requiring special agreements and protection.

(3) 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 IT3 personnel; and

b. Communicates the changes and updates to district stakeholders.

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