Administrative Procedures for Board Policy 05.51 Information Security & Privacy Program

05.51 AP.1	Asset Management (AST)
05.51 AP.11	Continuous Monitoring (MON)
05.51 AP.12	Cybersecurity Governance
05.51 AP.13	Security Awareness and Training
05.51 AP.14	Vulnerability

Asset Management (AST)

ASSET INVENTORIES 1

Control Objective: Physical devices and systems within the organization are inventoried, including:

- Assets with a property sticker identifying dollar amount of hardware $1,000 or greater.
- Software with a dollar amount greater than $5,000.

Procedure/Control Activity: Property Records Department manages and maintains an asset inventory within District software:

(1) Inventory Items are tracked starting with the Purchase Order and contain the following information:
    a. Hardware Inventory:
        i. Property Records tracks the asset at time of purchase and once received physically tags the device.
        ii. This information includes the location, date of purchase, date of retirement, and relevant asset details such as make and model number.
        iii. This process is state-mandated due to the need to report on public funds usage.

(2) Inventory management systems are updated continuously by automated.

ASSET INVENTORIES 2

Procedure/Control Activity: Software platforms and applications within the organization are inventoried. Property Records Department manages and maintains an asset inventory within the District inventory software system:

(1) Software inventory
    a. Current software approval process only tracks and maintains a history of software that has gone through the approval process or up for renewal.
    b. There is currently not a list of all in use software, nor is there a standardized or centralized repository for license keys for software. Software usage of District-approved software is tracked.

(2) Inventory management systems are updated in District inventory systems.

REMOVAL OF ASSETS

Procedure/Control Activity:
When an asset is to be retired:

(1) Authorization must be given from a supervisor or director for that location (e.g. Principal, School Technology Coordinator) that includes the reason for the retirement and removal of the asset.
(2) A ticketed request is completed and submitted.
(3) A surplus pickup form is required for collection of a device. The form includes:
    a. Make/model/serial # of the asset;
    b. Location the asset was retrieved from; and
    c. Asset Tag Number.
(4) An asset is then placed in a 999 status when it is retired, or its location is updated if it is returned to the IT warehouse. This is completed once the asset tag is collected and fully processed.
(5) Property records are updated in District software by property record auditors to remove the asset.

Continuous Monitoring (MON)

CONTINUOUS MONITORING

Procedure/Control Activity: Manager Digital Privacy and Cybersecurity, in conjunction with Administrator Cybersecurity and Infrastructure Services:

(1) Implements appropriate administrative means to ensure controls are sufficient for capturing, protecting and reviewing logs from all system components in accordance with District requirements to centrally manage and identify anomalies or suspicious activity. This includes:
   a. Reviewing the following, at least daily:
      i. Review security event in District monitoring software;
      ii. Logs of all system components that store, process, or transmit sensitive data, or that could impact the security of sensitive data;
      iii. Logs of all critical system components; and
      iv. Logs of all servers and system components that perform security functions. This includes, but is not limited to, District enterprise management systems;
   b. Reviewing logs of all other system components periodically based on the District's policies, procedures, and risk management strategy, as determined by the District's annual risk assessment; and
   c. Following up to address exceptions and anomalies identified during the review process.

(2) Develops processes for the timely detection and reporting of failures of security controls on critical systems or systems containing sensitive data, including but not limited to, failure of firewall and District enterprise monitoring systems.

(3) Develops processes to respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls include:
   a. Restoring security functions;
   b. Follow federal National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) core functions: Identify, Protect, Detect, Respond, Recover;
   c. Identifying and documenting the duration (date and time start to end) of the security failure;
   d. Identifying and documenting the cause(s) of failure, including the root cause, and documenting the remediation required to address the cause(s) of failure, including the root cause;
   e. Identifying and addressing any security issues that arose during the failure;
   f. Performing a risk assessment to determine whether further actions are required as a result of the security failure;
   g. Implementing controls to prevent cause of failure from reoccurring; and
   h. Resuming monitoring of security controls.

Continuous Monitoring (MON)

MONITORING REPORTING

Procedure/Control Activity: Administrator Cybersecurity and Infrastructure Services:

(1) Utilize state and District enterprise monitoring solutions;

(2) Use vendor-recommended settings and industry-recognized secure practices to automatically filter audit records for events of interest, based on selectable event criteria including geolocation, brute force attacks; and

(3) Generate reports that allow asset custodians and data/process owners to review potentially significant issues and/or incidents on the system generating the event.

ANOMALOUS BEHAVIOR

Procedure/Control Activity: Administrator Cybersecurity, in conjunction with Network Operations and Assistant Director Infrastructure Services:

(1) Uses vendor-recommended settings and industry-recognized secure practices to establish a general baseline of network operations and expected data flows for users and systems;

(2) Determines normal time-of-day and duration usage for system accounts;

(3) Determines normal geolocation and travel situations via District software;

(4) Monitors for atypical usage of system accounts; and

(5) Reports atypical activities in accordance with the District Incident Response Plan (IRP).

INSIDER THREATS

Procedure/Control Activity: Administrator Cybersecurity, in conjunction with the Human Resources Division (HR), and Assistant Director Infrastructure Services:

(1) Within legal guidelines, uses vendor-recommended settings and industry-recognized secure practices to broadly monitor internal personnel activity to detect potential cybersecurity incidents via District software systems: and

(2) Reports atypical activities in accordance with the District IRP.

THIRD-PARTY THREATS

Procedure/Control Activity: Assistant Director Infrastructure Services, in conjunction with Administrator Cybersecurity:

(1) Within legal guidelines, uses vendor-recommended settings and industry-recognized secure practices to monitor third-party service provider activity to detect potential cybersecurity incidents;

(2) Incorporate external threat monitoring including the federal Cybersecurity and Infrastructure Security Agency (CISA), Recorded Future, and Homeland Security, to increase awareness of potential cybersecurity incidents;

(3) Reports atypical activities in accordance with the District IRP.

Cybersecurity Governance

PUBLISHING SECURITY & PRIVACY POLICIES

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

(1) Analyzes federal National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and applicable statutory, regulatory and federal requirements to create a list of requirements that need to be addressed by the District's policies, procedures and standards.

(2) Publishes security policies on District website.

(3) On a yearly basis, analyzes the most current third-party risk assessment to determine appropriate coverage for the District's specific capabilities, based on people, processes and technology resources.

(4) Designs and documents the District's security policies and procedures in a consolidated document. These documents are maintained on the District website and updated when additions or changes are made.

(5) Receives written endorsement from the CIO, General Counsel, Information, Integration, and Innovation (IT3) Executive Risk Management Committee, and Board approval of all security policies and Board review of all security procedures.

(6) Disseminates the approved policies to all staff via public website and in electronic form to ensure all District personnel understand their applicable requirements.

(7) On an annual basis, the CIO, Manager Digital Privacy and Cybersecurity, Assistant Director Infrastructure Services, and General Counsel revises processes to address necessary changes and evolving cybersecurity conditions. Whenever the process is updated:

a. Distributes copies of the change to the Board;
b. Communicates the changes and updates to District staff; and
c. Makes changes to the District website.

ASSIGNED SECURITY RESPONSIBILITIES

Procedure/Control Activity: The Human Resources Division (HR), in conjunction with the Manager Digital Privacy and Cybersecurity, CIO, and General Counsel:

(1) The District leverages the NIST CSF and National Initiative for Cybersecurity Education (NICE) for identifying necessary roles and responsibilities. The Manager Digital Privacy and Cybersecurity and CIO:

a. Maintains a Computer Security Incident Response Team (CSIRT) composed of cybersecurity analysts;
b. Establishes, documents and distributes security policies and procedures maintained by the CSIRT Team on the District website;
c. The IT3 CSIRT Team monitors and analyzes security alerts and information via cloud-based management tools;
d. Distribute and escalate security alerts to appropriate personnel including the CSIRT Team, local law enforcement and federal officials as needed;

Cybersecurity Governance

ASSIGNED SECURITY RESPONSIBILITIES (CONTINUED)

e. Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. Incident reports are centrally located and accessed by the CSIRT team from a repository that is private to only IT3 CSIRT staff;
f. Infrastructure services team administer user accounts, including additions, deletions and modifications; and
g. Infrastructure services team monitors and controls access to data.

(2) Utilizes existing HR and IT3 processes to assign formal roles and responsibilities to employees who have cybersecurity job functions. Create separate administrator accounts with Multi-Factor Authentication (MFA) enforced for all administrative functions.

(3) Provides written notification to the employee of assigned cybersecurity roles and responsibilities in employment contract yearly.

(4) Review on an annual basis, prior to contract signature for the school year or as needed, any revisions to processes to address necessary changes and evolving conditions. Whenever the process is updated:

a. Distributes copies of the change to employee, HR staff, and CIO; and
b. Communicates the changes and updates to appropriate IT3 leaders.

MEASURES OF PERFORMANCE

Procedure/Control Activity

CIO, in conjunction with Manager Digital Privacy and Cybersecurity, Assistant Director Infrastructure Services, HR, and General Counsel:

(1) Based on the District's implementation of the NIST CSF, develops measures of performance or outcome-based metrics to measure the effectiveness or efficiency of the controls employed across the District.

(2) Communicates awareness and understanding of completion metrics to HR.

(3) Creates and manages a process to share the effectiveness of protection technologies with appropriate stakeholders including security awareness reports and training requirements. Implementation of security awareness training and mandating cybersecurity training modules including the core NIST CSF components and federal trainings regarding the Health Insurance Portability and Privacy Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and personal identifying information (PII).

(4) On an annual basis, prior to contract signature, reviews the process for non-conforming instances of security training. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:

a. Distributes copies of the changes to HR; and
b. Communicates the changes and updates to key personnel including Chief of HR, General Counsel, and the CIO.

Security Awareness and Training

SECURITY & PRIVACY TRAINING

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

(1) Use industry-recognized practices to ensure security training that consists of:
   a. All employees sign an Acceptable Use Policy (AUP) stating they have read and understand the District's requirements regarding cybersecurity policies, standards, procedures and guidelines prior to having access to District systems or data;
   b. All employees are required to complete online security awareness training classes within thirty (30) days of being granted access to any system;
   c. All users undergo online security awareness training annually via online platform; and
   d. All users are provided with sufficient training and supporting reference materials to allow them to properly protect the District's systems and data;

(2) Work with District management to develop and maintain a communications process to be able to communicate new cybersecurity and privacy program information, such as an informational security bulletin or email about security items of interest; and

(3) On an annual basis, work with the HR Division to review the processes for non-conforming instances, and, as needed revise processes to implement necessary changes and address evolving conditions.

PRIVILEGED USERS

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

(1) Implement appropriate administrative measures to ensure that every privileged user is provided specific training to ensure privileged users understand their roles and responsibilities, including measures to ensure:
   a. Individuals acknowledge responsibilities in writing before permission is granted;
   b. Privileged accounts are requested by a service ticket; and
   c. Accounts are reviewed for login activity. Accounts not logged into for ninety (90) days are marked inactive.

SECURITY & PRIVACY-MINDED WORKFORCE

Procedure/Control Activity: Compliance, HR, Manager Digital Privacy and Cybersecurity, Assistant Director Infrastructure Services:

(1) Create and implement:
   a. A formal, documented security awareness training course for all staff with administrative or elevated privileges that includes:
      i. Defining the knowledge and skill levels needed to perform cybersecurity duties and tasks;
      ii. Developing role-based training programs for individuals assigned cybersecurity roles and responsibilities;
      iii. Providing standards for measuring and building individual qualifications for incumbents and applicants for cybersecurity-related positions as defined in the National Initiative for Cybersecurity Education (NICE);

Security Awareness and Training

SECURITY & PRIVACY-MINDED WORKFORCE (CONTINUED)

b. Processes to facilitate the implementation of awareness training and regular updates that cover policies, procedures and processes relating to a user's professional function as it pertains to the District; and
c. On at least an annual basis, Infrastructure Services and the Manager Digital Privacy and Cybersecurity Manager review the process for non-conforming instances. As needed, they revise processes to address necessary changes and evolving conditions.

Vulnerability

VULNERABILITY & PATCH MANAGEMENT PROGRAM

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

(1) Use vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for managing an enterprise-wide technical Vulnerability & Patch Management Program that utilizes a risk-based model for prioritizing remediation of identified vulnerabilities;

(2) Deploy approved updates for all desktop devices and servers;

(3) Ensure that mobile devices are maintained via District mobile device management (MDM) solution;

(4) Ensure that Zero-Day exploits (imminent threats) are identified and patched immediately;

(5) On at least an annual basis, review the third-party vulnerability test to assess for non-conforming instances. As needed, processes are revised to implement necessary changes and address evolving conditions;

(6) Whenever a process is updated:

a. Distribute copies of the change to Assistant Director Infrastructure Services and Manager Digital Privacy and Cybersecurity; and
b. Communicate the changes and updates to appropriate District leadership and stakeholders.

CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES

Procedure/Control Activity: Administrator Cybersecurity, in conjunction with Infrastructure Services, implements appropriate administrative means to ensure District-owned devices address applicable threats by conducting proactive reviews of systems and applications for vulnerabilities and misconfigurations through:

(1) Utilizing vulnerability assessment tools or methods. At least monthly, update workstations and servers with approved patches, including:

a. Where technically feasible and justified by a valid business case, continually checking all connections;
b. Patching Zero Day vulnerabilities immediately after testing; and
c. Deploying third party vendor patches after successful internal testing

(2) Follow District change control processes to ensure remediation steps are conducted, in accordance with the District Change Management process; and

(3) On at least an annual basis, reviews the third-party risk assessment and vulnerability assessments for non-conforming devices.

VULNERABILITY SCANNING

Procedure/Control Activity: Chief Information Officer (CIO), Manager Digital Privacy and Cybersecurity, Assistant Director Infrastructure Services, in conjunction with the Cybersecurity Team, implements appropriate administrative means to ensure authorized external, third party conduct the following vulnerability scanning-related activities:

Vulnerability

(1) Perform ongoing scans for vulnerabilities in systems and hosted applications, as well as ad hoc scans when a new vulnerability potentially affecting a system or application is identified and reported in District domains, utilizing patch management and vulnerability identification software.

   a. Utilize vulnerability scanning tools and techniques that promote:
      i. Enumerating platforms, software flaws, and improper configurations;
      ii. Formatting and making transparent checklists and test procedures; and
      iii. Measuring vulnerability impact;
   b. Analyze vulnerability scan reports and results;
   c. Remediate legitimate vulnerabilities in accordance with a risk-based approach using approved updates; and
   d. Share information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the District to help eliminate similar vulnerabilities in other systems;

(2) On an annual basis, review the third-party vulnerability scan. As needed, revise processes to implement necessary changes and address evolving conditions; and.

(3) Whenever a process is updated, communicate the changes and updates to the Assistant Director Infrastructure Services and the CIO.

RED TEAM EXERCISES

(Specifically not a National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Control or function by itself)

Procedure/Control Activity: The District does not employ "red team" members and relies on external third-party entities for vulnerability assessments. Manager Digital Privacy and Cybersecurity, in conjunction with the Director Internal Audit and Infrastructure Services:

(1) Implements appropriate physical, administrative and technical means to coordinate for "red team" penetration testing exercises that are intended validate the District's ability to defend against, detect and respond to directed cybersecurity attacks;

(2) Utilizes industry-recognized practices for conducting penetration testing by either internal or third-party penetration testing specialists; and

(3) Provides a formal report on the results of the red team exercise upon the conclusion of the exercise to all key stakeholders so that "lessons learned" activities can be conducted to update protection, detection and response capabilities.