Physical & Environmental Security (PES)

NIST CSF PR.AC-2 Physical Access Control

Procedure/Control Activity:

(1) Follows appropriate industry-expected guidelines to implement and govern physical security controls, in accordance with Board policies, District administrative procedures, and standards implemented.
(2) Enforces physical access authorizations for all physical access points (including designated entry/exit points) to District-owned or operated facilities.
(3) Verifies individual access authorizations before granting access to the facility.
(4) Controls access to areas based on the physical security zone requirements.
(5) Secures keys, combinations, and other physical access devices.
(6) Changes or replaces combinations and keys when keys are lost, combinations are compromised, or when an employee is transferred or is no longer employed by the District .
(7) Issues a visitor a physical token (e.g., a badge or access device) that:
    a. Identifies the visitor as being not an onsite employee;
    b. Is surrendered by the visitor before leaving the facility or at the date of expiration; and
    c. Expires through automated or visual means (e.g., different color for each day, date/time on school provided name badge, etc..).
(8) On at least an annual basis, review the process for non-conforming instances. As needed, revise processes to address necessary changes and evolving conditions. Whenever a process is updated:
    a. Distribute copies of the change to key District personnel; and
    b. Communicate the changes and updates to key District personnel.
(9) If necessary, request corrective action to address identified deficiencies.
(10) If necessary, validate that corrective action occurred to appropriately remediate deficiencies.
(11) If necessary, document the results of corrective action and note findings.

NIST CSF DE.CM-2 Monitoring Physical Access

Procedure/Control Activity:

(1) Follows appropriate industry-expected practices to perform physical access monitoring, in accordance with Board policies, District administrative procedures, and standards, including:
    a. Using video cameras, surveillance equipment and/or physical access control mechanisms to monitor individual physical access to sensitive areas;
    b. Investigating and responding to detected physical security incidents, per documented procedures;
    c. Performing security checks at the physical boundary of the facility or system for unauthorized exfiltration of information or system components;
    d. Reviewing collected data and correlating with other entries; and
    e. Retaining physical access data for at least three (3) months, unless otherwise restricted by law.
(2) On at least an annual basis, reviews 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 District personnel; and
    b. Communicate the changes and updates to key District personnel.
(3) If necessary, request corrective action to address identified deficiencies.
(4) If necessary, validate that corrective action occurred to appropriately remediate deficiencies.
(5) If necessary, document the results of corrective action and note findings.

Physical & Environmental Security (PES)

NIST CSF PR.DS-5 Information Leakage Due To Electromagnetic Signal Emanations

Procedure/Control Activity:

(1) Implements appropriate physical, administrative and technical means to secure facilities to reduce the chance of information leakage due to electromagnetic signal emanations through:
   a. The proper placement of Wireless Access Points (WAPs);
   b. Limiting the output/transmission power of the WAPs; and
   c. Ensuring users are educated about positioning monitors to minimize the risk of unauthorized individuals being able to intentionally or inadvertently view the screen.

(2) On at least an annual basis, 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 District personnel; and
   b. Communicate the changes and updates to key District personnel.

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

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

(5) If necessary, document the results of corrective action and note findings.

Risk Management

NIST CSF ID.GV-4: RISK MANAGEMENT PROGRAM

Procedure/Control Activity:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for managing risk that include:
   a. A formal Risk Management Program (RMP) that includes:
      i. An unambiguous expression of the risk tolerance;
      ii. Acceptable risk assessment methodologies; and
      iii. Risk mitigation strategies.
   b. A process for consistently evaluating and monitoring risk over time;
   c. A process for conducting risk assessments annually and upon significant changes to the district environment;
   d. Identification of:
      i. Critical assets;
      ii. Current safeguards; and
      iii. Effectiveness of safeguards against threats and vulnerabilities.
   e. A review of processes involving creating, receiving, maintaining and transmitting of sensitive data; and
   f. Assignment of responsibility to validate security controls.

(2) As needed, revise processes to address necessary changes and evolving conditions. Whenever a process is updated:
   a. Distribute copies of the change to key District personnel; and
   b. Communicate the changes and updates to key District personnel.

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

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

(5) If necessary, document the results of corrective action and note findings.

NIST CSF ID.RA-3: Risk Identification

Procedure/Control Activity:

(1) Implements appropriate administrative means to leverage the district's Risk Management Program (RMP) to identify, document and report risk.
(2) As needed, revise risk profile to address necessary changes.
(3) As needed, revise processes to address necessary changes and evolving conditions. Whenever a process is updated:
    a. Distribute copies of the change to key District personnel; and
    b. Communicate the changes and updates to key District personnel.
(4) If necessary, request corrective action to address identified deficiencies.
(5) If necessary, validate that corrective action occurred to appropriately remediate deficiencies.
(6) If necessary, document the results of corrective action and note findings.

NIST CSF ID.RA-6 RISK REMEDIATION

Procedure/Control Activity:

(1) Implements appropriate administrative means to leverage the appropriate Risk Management Program (RMP) to:
    a. Mitigate risks to an acceptable level; or
    b. Conduct remediation actions, based on risk criteria, in accordance with reasonable resolution time frames and stakeholder approval.

(2) On at least an annual basis, review the process for non-conforming instances. As needed, revise processes to address necessary changes and evolving conditions. Whenever a process is updated:
    a. Distribute copies of the change to key District personnel; and
    b. Communicate the changes and updates to key District personnel.

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

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

NIST CSF ID.RA-4 BUSINESS IMPACT ANALYSIS (BIAS)

Procedure/Control Activity:

(1) Implements appropriate administrative means to utilize a defined and documented method for determining the impact of any disruption to the district's business operations (e.g., Business Impact Analysis (BIA)) that incorporates the following:
   a. Identifies critical products and services;
   b. Identifies all dependencies, including processes, applications, business partners, and third-party service providers;
   c. Understands threats to critical products and services;
   d. Determines impacts resulting from planned or unplanned disruptions and how these vary over time;
   e. Establishes the maximum tolerable period of disruption;
   f. Establishes priorities for recovery;
   g. Establishes recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption; and
   h. Estimates the resources required for resumption.

(2) On at least an annual basis, review the process for non-conforming instances. As needed, revise processes to address necessary changes and evolving conditions. Whenever a process is updated:
   a. Distribute copies of the change to key District personnel; and
   b. Communicate the changes and updates to key District personnel.

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

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

Secure Engineering & Architecture (SE)

NIST CSF PR.IP-1 SECURE ENGINEERING PRINCIPLES

Procedure/Control Activity:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for applying industry-recognized secure practices engineering principles in the specification, design, development, implementation, and modification of systems. These include:
   a. Implementing configuration standards for all system components that address known security vulnerabilities and are consistent with industry-accepted system hardening standards;
   b. Developing layered protections;
   c. Establishing sound security architecture and controls as the foundation for design;
   d. Incorporating security requirements into the Secure Development Life Cycle (SDLC);
   e. Delineating physical and logical security boundaries;
   f. Ensuring system developers are trained on how to build secure software;
   g. Tailoring security controls to meet organizational and operational needs;
   h. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and
   i. Reducing risk to acceptable levels, thus enabling informed risk management decisions.

(2) On at least an annual basis, review the process for non-conforming instances. As needed, revise processes to address necessary changes and evolving conditions. Whenever a process is updated:
   a. Distribute copies of the change to key District personnel; and
   b. Communicate the changes and updates to key District personnel.

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

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

NIST CSF PR.PT-5 FAIL SECURE

Procedure/Control Activity:

(1) Uses vendor-recommended settings and industry-recognized secure practices to configure critical assets to fail in a known state or safe mode in order to preserve system state information at the time of the failure if possible.

(2) On at least an annual basis, 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 District personnel; and
   b. Communicate the changes and updates to key District personnel.

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

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