Business Continuity and Disaster Recovery (BCD)

NIST CSF RC.RP-1 CONTINGENCY PLAN

Procedure/Control Activity:

(1) Use industry-recognized secure practices to develop a contingency plan that:

a. Identifies essential missions and business functions and associated contingency requirements;

b. Provides recovery objectives, restoration priorities, and metrics;

c. Addresses contingency roles, responsibilities, assigned individuals with contact information;

d. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;

e. Addresses eventual, full system restoration without deterioration of the security measures originally planned and implemented;

f. Is reviewed and approved by Division management; and

g. Is coordinated with incident handling activities.

(2) Establish processes for obtaining access to sensitive data during other-than-normal or emergency conditions.

(3) On at least an annual basis, review the contingency plan.

(4) 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.

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

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

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

NIST CSF RC.IM-1 CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED

Procedure/Control Activity:

(1) Perform a Root Cause Analysis (RCA) following events that trigger usage of continuity plans.

(2) Incorporate lessons learned in updates to the applicable Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

(3) 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:

Business Continuity and Disaster Recovery (BCD)

NIST CSF RC.IM-1 CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED

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 RC.IM-2 CONTINGENCY PLAN UPDATE

Procedure/Control Activity:

(1) On at least an annual basis:

a. Review the contingency plan;

b. Review any test/exercise results; and

c. Validate that lessons learned were incorporated in updates to the applicable Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

(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.

Compliance (CPL)

NIST CSF PR.IP-7 STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE

Procedure/Control Activity:

(1) Implement appropriate administrative means to document the geographic location of all District facilities.

(2) Utilize online resources to identify changes in statutory and/or regulatory data protection requirements that impact all geographical locations, including but not limited to:

a. **US States** - http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx

b. **US Federal** - https://content.next.westlaw.com/Browse/Home/PracticalLaw

c. **International** - https://www.dlapiperdataprotection.com

(3) Consult with the Office of the General Counsel to determine if there are any new contractual obligation changes.

(4) Document any changes to statutory, regulatory, and contractual compliance obligations.

(5) Assemble key stakeholders to perform a review of District policies, administrative procedures, processes, and standards to address necessary changes, if necessary.

(6) Incorporate feedback into an updated version of District policies, administrative procedures, processes, and standards.

(7) On at least an annual basis, oversee the change management process to release the changes from draft into production.

(8) 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.DP-5 SECURITY CONTROLS OVERSIGHT

Procedure:

(1) Develop and maintain a cybersecurity governance program that will:

a. Take into account:

i. Applicable statutory, regulatory, Board policy, and contractual requirements;

ii. Industry-specific trends that impact District's cybersecurity expectations; and

Compliance (CPL)

NIST CSF DE.DP-5 SECURITY CONTROLS OVERSIGHT (CONTINUED)

iii. Historical trends within the District that have had an impact on cybersecurity operations;

b. Establish:

i. Key Performance Indicators (KPIs); and

ii. Key Risk Indicators (KRIs); and

c. Assign the task of establishing a Continuous Monitoring (CM) capability to provide oversight to ensure that the District's cybersecurity controls are both in-place and operational.

(2) On at least an annual basis, review the process for non-conforming instances. As needed, revises 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.

Data Classification and Handling (DCH)

NIST CSF PR.IP-6 PHYSICAL MEDIAL DISPOSAL

Procedure:

(1) Use industry-recognized secure practices to implement retention practices for data, based on the District's records retention standards in accordance with Board Policy 01.61 and Kentucky Administrative Regulation Chapter 725.

(2) Dispose of media when it is no longer necessary for business, legal, financial, or historical purposes, and in accordance with the Kentucky Public School District Records Retention Schedule incorporated by reference in 725 KAR 01.061.

(3) The method of destruction for media follows one of the following methods, based on the type of media:

a. Physical Paper-Based Media:

Physical Paper-Based Media (e.g., accounts payables, accounts receivables, Special Education student files, etc.) are destroyed to make sensitive data technically impossible to recover;

i. The process of shredding is performed internally or outsourced to a trusted third-party that specializes in document destruction;

ii. Physical paper-based media containing non-sensitive data is shredded but can be recycled; and

iii. Physical paper-based media containing sensitive data (e.g., SSNs, financial information, client communications, etc.) is shredded, incinerated, or pulped so that data cannot be reconstructed.

b. Physical Digital Media:

Physical digital media (e.g., Hard Disk Drives (HDDs), flash drives, floppy drives, tape drives, etc.) are destroyed to make recovery of data technically impossible;

i. The process of destruction is outsourced to a trusted third-party that specializes in the physical destruction of digital media;

ii. HDDs are removed from all systems, prior to the disposal of the system;

iii. Outsourced destruction vendors track HDDs by serial number to ensure the secure destruction of the devices; and

iv. Records of media destruction are retained in accordance with retention schedules.

c. Electronic Digital Media:

Electronic Digital Media (e.g., Files, Databases, Email, Spreadsheets, etc.) are destroyed to make recovery of data technically impossible;

i. The process of destruction for electronic media contained in cloud storage is to delete the media without retaining a copy.

Data Classification and Handling (DCH)

NIST CSF PR.IP-6 PHYSICAL MEDIAL DISPOSAL (CONTINUED)

ii. The process of destruction for electronic media contained on a local or removable drive (e.g., HDD located in a tablet, PC, laptop, server, a thumb drive, external harddrive, etc.) is to delete the media without retaining a copy.

iii. The process of destruction for local or removable electronic media is to use industry-recognized standards (e.g., degaussing, cryptoshredding, physical shredding, sanitation, etc.) to make the recovery of data technically impossible.

(4) 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:

c. Distribute copies of the change to key District personnel; and

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

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

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

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

NIST CSF PR.PT-2 Removable Media Security

Procedure:

(1) Implement appropriate physical, administrative, and technical means to ensure compel end users to adhere to the District's data handling requirements for removable media.

(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.

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

Incident Response Operations (IRO)

NIST CSF PR.IP-9 Incident Response Operations

Procedure/Control Activities:

(1) Through the use of vendor-recommended settings and industry-recognized secure practices, ensure controls are sufficient for managing enterprise-wide incident response that includes:

a. A formal, documented Incident Response Plan (IRP); and

b. A defined process to facilitate and implement the incident response process and associated controls.

(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.

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

P-IRO-02: Incident Handling

Procedure/Control Activities:

(1) Leverage the appropriate Incident Response Program to:

a. Investigate possible incidents detected.

b. Identify and assess the severity and classification of incidents.

c. Define appropriate actions to take in response to an incident, in accordance with the appropriate Incident Response Plan (IRP).

d. Respond with appropriate remediation actions to minimize impact and ensure the continuation of business functions.

e. As necessary, update the IRP, based on lessons learned from an incident.

(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.

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

Network Security (NET)

NIST CSF PR.PT-4 Network Security Management

Procedure/Control Activities:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for protecting communications and networks, including:

a. Administrative controls that govern changes to the environment;

b. Technical controls that provide a defense-in-depth approach; and

c. Network services agreements, whether these services are provided in-house or outsourced to trusted third parties.

(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.

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

Identification and Authentication (AIC)

NIST CSF PR.AC-6 USER PROVISIONING & DE-PROVISIONING

Procedure/Control Activities:

(1) Implement appropriate administrative and technical means to ensure controls are sufficient for implementing and managing a formal user access provisioning process to assign and/or revoke access rights for all user types to all systems and services by:

a. Provisioning user access (e.g., employees, students, contractors, customers [tenants], business partners, and/or supplier relationships) to data and organizationally owned or managed (physical and virtual) applications, infrastructure systems, and network components;

b. Ensuring that user access is authorized by District management prior to access being granted; and

c. Implementing timely de-provisioning (revocation or modification) of user access to data and District -owned or -managed (physical and virtual) applications, infrastructure systems, and network components:

i. In accordance with established procedures and processes; and

ii. Based on user's change in status, including, but not limited to:

1. Termination of employment, job change, or transfer;

2. Termination of or change to a business relationship;

3. Termination of or change to a student enrollment).

(2) On at least an annual basis, review the processes 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.

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

NIST CSF PR.AC-1 ACCOUNT MANAGEMENT

Procedure/Control Activities:

(1) Use vendor-recommended settings and industry-recognized secure practices to ensure proper user identification and authentication management for all standard and privileged users on systems by:

a. Controlling the addition, deletion, and modification of user IDs, credentials, and other identifier objects to ensure authorized use is maintained;

b. Verifying user identity before issuing initial passwords or performing password resets;

Identification and Authentication (AIC)

NIST CSF PR.AC-1 ACCOUNT MANAGEMENT (CONTINUED)

c. Revoking access for any terminated users in a timely manner;

d. Removing/disabling inactive user accounts in a timely manner;

e. Using industry standard hardening techniques to enhance account security;

f. Establishing and administering accounts in accordance with a role-based access scheme that organizes system and network privileges into roles, if applicable;

g. Tracking and monitoring role assignments for privileged user accounts, if applicable;

h. Terminating access for temporary and emergency accounts after the accounts are no longer needed in a timely manner;

i. Minimizing the use of group, shared, or generic accounts and passwords;

j. Disabling or removing default user IDs and accounts where applicable;

k. Forcing service providers with remote access to District systems to use a unique authentication credential (such as a password/phrase) for each user; and

l. Restricting user direct access or queries to databases to database administrators if applicable, including:

i. Verifying that database and application configuration settings ensure that all user access to, user queries of, and user actions on (e.g., move, copy, delete), the database are through programmatic methods only (e.g., through stored procedures);

ii. Verifying that database and application configuration settings restrict user direct access or queries to databases to database administrators; and

iii. Reviewing database applications and the related application IDs to verify that application IDs can only be used by the applications and not by individual users or other processes.

(2) On at least an annual basis, review the procedure 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.

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

Identification and Authentication (AIC)

NIST CSF PR.AC-4 Least Privilege

Procedure/Control Activities:

(1) Use vendor-recommended settings and industry-recognized secure practices to implement the "principle of least privilege," which states that only the minimum access necessary to perform an operation should be granted.

(2) Grant access only for the minimum:

a. Levels of permissions necessary to perform the job function; and

b. Time required.

(3) On at least an annual basis, review the procedure 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.

(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.

Endpoint Security (END)

NIST CSF DE.CM-4 MALICIOUS CODE PROTECTION (ANTI-MALWARE)

Procedure/Control Activities:

(1) Use vendor-recommended settings and industry-recognized secure practices to deploy District and state-approved anti-malware software on all systems capable of running anti-malware software, including, but not limited to:

a. Workstations;

b. Servers;

c. Tablets; and

d. Mobile devices.

(2) Ensure logs alert incident response personnel upon detection of malware or possible threats.

(3) Implement appropriate administrative means to ensure that anti-malware software is capable of detecting, removing, and protecting against all known types of malware.

(4) Perform periodic evaluations to identify and evaluate evolving malware threats on information systems considered to be not commonly affected by malware, in order to confirm whether such information systems continue to not require anti-malware software.

(5) Document business justification for systems not capable of running anti-malware software and what compensating controls are in place to minimize the risk associated with the lack of anti-malware software on that system.

(6) 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.

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

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

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