Document Status: Draft

AR Required: No

AR 3522 DISTRICT DATA PROTECTION PROGRAM

Note: This District Data Protection Program (DDPP) was developed by utilizing the National Institute of Standards and Technology (NIST) Common Security Framework (CSF). The following administrative regulation describes the framework and an outline of how a program may be implemented. This regulation may be modified to fit district needs.

Introduction

The District Information Technology (IT) Department (or contracted services) has a responsibility to protect sensitive District data to include financial, employee, and student data, while allowing for a positive learning environment. The objective is to employ technology resources that create equitable and accessible learning systems that make learning possible everywhere and all the time.

Section 1. Responsibilities

The District is responsible for providing the following activities in support of the District's data protection program:

Superintendent

- Superintendent periodically reports to the board regarding the function and performance of the DDPP.
- Shall appoint a Data Protection Leader (see activities below) who will provide an annual risk assessment to the board in support of a separate District Data Protection Program.
    - The designated Data Protection Leader shall have sufficient decision-making capabilities to effectively manage all aspects of the DDPP to include:
- Executing emergency contracts in the event of a data breach.
- Directing staff/faculty activities as required in support of the DDPP.
- Directing or implementing changes to the network/operating environment as required. Provide incident information to Human Resources as needed. '
- Shall participate in one "tabletop" disaster recovery exercise per year wherein a cybersecurity incident is simulated, and receive the report on the outcome of the exercise.
- Shall review an annual risk assessment and provide comments to the Data Protection Leader as required.
- Shall prepare a separately itemized annual security budget.

Data Protection Leader

- Shall be formally recognized as the District's Data Protection Program Leader.
- Shall be responsible for the design, architecture, implementation, program management and oversight of the DDPP on behalf of the District.

- Shall ensure that an annual Risk Assessment is prepared and delivered to the
- Superintendent in support of an Annual Security Budget Request.
- Shall be responsible for the maintenance and dissemination of all required security documentation to include training records, plans, policies, procedures, configurations, and standards applicable to the DDPP.
- Be responsible for conducting an annual tabletop exercise with the leadership simulating a Data Security Breach.
- Ensuring a successful restore from data backups on a quarterly basis.
- Shall lead annual security training for all staff and District personnel and maintain all training records as required.

Staff and Faculty

- Shall be responsible for completing all security training assignments in a timely manner.
- Maintaining all data in their purview in the manner directed by the Data Protection Leader.
- Reporting security incidents and problems in accordance with District policies and procedures.
- Comply with the District data security policies and procedures.

Section 2. Framework

The District recognizes an effective data protection program is essential to protecting sensitive data and ensuring information technology enables a rich learning environment. The District Data Protection Leader is responsible for recommending and implementing appropriate controls to protect District information and resources. The data protection framework will employ a layered defense strategy with protocols to prevent, detect, and respond to potential threats. The core framework shall be implemented through a combination of Department people, processes, and technologies capable of meeting the requirements and standards. In addition, the Data Protection Leader will develop and maintain a District knowledge base that will act as a document and information repository for all District data protection related information. The following sections outline the core governance framework for the DDPP.

- Data ProtectionGovernance
- Training
- Network Security
- Endpoint Security
- Application Security
- Data Security
- Identity & Access Management

Section 3. Data Protection Governance

The Data Protection Leader shall establish a governance structure to ensure the confidentiality, integrity, and availability of District systems and data. The Data Protection Leader shall maintain an electronic document repository with all required procedures, guidelines, and checklists including the following elements:

- **Data Protection Plan** – Develop and implement a DDPP that provides an overview of District data protection requirements and describes the controls, responsibilities, and expected behavior of individuals who access various systems. It shall include a 1-page training addendum outlining the training

requirements, tools, and calendar. The Data Protection. Leader shall update the DDPP annually.

- **Incident Response Plan** – Develop and establish an incident response plan that provides a set of instructions to help staff detect, respond to, and recover from network security incidents and document the approved recovery process. The Data Protection Leader shall update the incident response plan annually.

Section 4. Training

The Data Protection Leader shall implement a district-cybersecurity training program that is comprised of static and interactive cybersecurity training. The program will be designed to deliver a yearly training event at a minimum. The training program shall include at a minimum the following elements:

- **Training records** for all events that track who took the training, how they performed during the training and any remedial actions that were required.
- **Deliver an annual organization wide synchronous training** identifying the following:
  - The Data Protection Leader
  - Critical program standards
  - What to do in the event of a disaster or security incident
  - Attendance will be included in the report
- **Interactive Cybersecurity Training** may include but is not limited to:
  - Phishing testing
  - Social engineering testing
  - Games
  - Awareness posters
  - Integrated into in-service and continuing education processes
  - Videos

Section 5. Network Security

The Data Protection Leader shall implement adequate policies, procedures, and technical controls to protect the security of the network to include the following elements at a minimum:

- **Perimeter Security** – Develop and deploy network security devices and tools in such a manner as to ensure District data is appropriately protected from unauthorized use or access.
- **Network Design Documentation** – Develop and update network diagrams as needed and should include the following information at a minimum:
  - All entry points from the Internet
  - All firewalls, switches, routers, and wireless access points
  - Type, size, and bandwidth of all connections
  - External IP address and Internal virtual local area networks (VLANs)
  - Externally connected systems
- **Firewall Security** – Ensure the firewall configuration is documented and configured in accordance with District requirements. Policies for firewall rule changes, audit logging, and monitoring and managing perimeter and internal firewalls must be established and maintained at all times.
- **Remote Access** – Establish a secure process and deploy effective controls for remote access to District resources and. monitor remote access through approved monitoring tools to prevent unauthorized access.
- **Router and Switch Security** – Develop standards and configure routers and switches in accordance with best practices. Switch and router configurations shall

be backed up as needed and routine audits should be conducted to ensure configurations are correct.

- **Wireless Security** – Enable and secure District wireless access points and networks in accordance with industry and manufacturer best practices.
- **Internet Use** – Will be monitored and manage in accordance with a District Internet Use policy and at a minimum filtered in accordance with legal requirements such as CIPA, HIPPA, etc.
- **Network Monitoring** – The District must maintain an appropriate network monitoring capability to detect, identify, respond, and recover from network security events.
- **Vulnerability & Patch Management** – The District must develop and maintain an effective vulnerability and patch management process. This process shall include capabilities to scan the network for vulnerabilities and ensure appropriate system/software patches have been implemented.
- **Ports & Protocols** – The must develop and maintain a ports and protocols list to include permissible and blocked ports and protocols.

Section 6. Endpoint Security

The Data Protection Leader shall implement adequate policies, procedures, and technical controls that require endpoint device compliance before they are granted access to network resources. At a minimum the program will include:

- **Mobile Device Management** – Deploy network security devices and tools in such a manner to ensure District data is appropriately protected from unauthorized use or access and can be remotely managed.
- **Anti-Virus Protection** – Deploy effective anti-virus protection throughout the District. Update and monitor this program routinely.
- **Vulnerability & Patch Management** – Develop and maintain an effective vulnerability and patch management process. Include capabilities to scan endpoints for vulnerabilities and implement appropriate system/software patches.
- **Endpoint Monitoring** – Assess and deploy an endpoint solution that addresses malware exploits by observing attack techniques and behaviors. Coordinate enforcement with network and cloud security to prevent successful attacks.

Section 7. Application Security

The Data Protection Leader shall implement adequate policies, procedures, and technical controls that enable application security. At a minimum the program will include:

- **Software Inventory** – The Data Protection Leader shall develop and maintain a software inventory of applications, systems, and databases for the District.
- **Application Access Management** – The Data Protection Leader shall work with system owners to ensure appropriate application access controls are in place to protect information.
- **Data at Rest** – The Data Protection Leader shall implement data at rest controls as deemed appropriate in support of the District's risk appetite.

Section 8. Data Security

The Data Protection Leader shall implement appropriate policies and technical and physical controls to protect sensitive data. The Data Protection Leader shall work with data owners to identify sensitive data and implement controls to allow for the timely

detection, response, and recovery of unauthorized access or handling of sensitive data. At a minimum the program:

- **Cloud Security** – Shall develop and maintain a process for managing all cloud applications and identifying the types of data being stored.
- **Data Backup** – Shall develop, implement, and maintain data backup support based on coordinated Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) and outline off-site and off-line backup requirements.
- **Data in Transit** – Shall consider data in transit controls as deemed appropriate. Account for and maintain the specific controls for externally managed systems accessed by the district in the normal course of business. Examples of this may include the Criminal Justice Information Services (CJIS) which requires the Data Protection Leader to work with a Local Agency SecurityOfficer (LASO) to implement compliant security measures and procedures.

Section 9. Identity & Access Management

The Data Protection Leader shall implement adequate policies, procedures, and technical controls that comply with an established framework, such as NIST, and/or best practices. At a minimum the program will:

- **User Management** – Develop and maintain a directory service to manage user access to various IT resources such as systems, devices, applications, storage systems, and networks. The directory service and associated automation should enable admins to control user access and on-board and off-board users to and from IT resources. The directory service must authenticate, authorize, and audit user access to IT resources.
- **Privileged Account Management** – Ensure appropriate application/system access controls for various applications, systems, and network administrators.
- **Least Privilege** – Implement the principle of least privilege across the enterprise.
- **Access Controls** – Implement district-wide role-based access controls.
- **Multi-Factor Authentication** – Assess and deploy multi-factor authentication as deemed appropriate.

(*cf. 1340 and AR 1340* - Access to District Records)

(*cf. 3580 and AR 3580* - District Records)

(*cf. 3523* and AR 3523 - Employee Use of District Information Technology)

(*cf. 3523.1 and AR 3523.1* - Blogging)

(*cf. 3523.2 and AR 3523.2* - Social Media Use)

(*cf. 4112.6* - Personnel Records)

(*cf. 4119.23* - Unauthorized Release of Confidential Information)

(*cf. 4119.25 and AR 4119.25* - Political Activities of Employees)

(*cf. 4419.5* - Electronic Communications Between Employees and Students)

(*cf. 5125* - Student Records)
(*cf. 5145* - Anti-Bullying/Anti-Cyberbullying)

(*cf. 6161.4* - Student Use of District Information Technology)

~~Legal References:~~

~~47 U.S.C. 201 *et seq.*, Communications Decency Act of 1995, as amended.~~

~~20 U.S.C. 1232g., Federal Family Educational Rights and Privacy Act of 1974, as amended. 47 U.S.C. 231 *et seq.*, Children's Online Privacy Protection Act of 2000, as amended. *Adopted 4/2022*~~

~~AASB POLICYREFERENCE MANUAL~~

~~9/92~~