ADMINISTRATIVE REGULATION

APPROVED:

REVISED:

830.1-AR-0. DATA STORAGE AND SECURITY

The district will take action to safeguard the integrity of the data and information collected, created, stored and managed by the district through the maintenance, review and update of data storage and security procedures and disaster recovery plans.

The Superintendent, Business Manager and Director of Information Technology will ensure the proper segregation of duties in assigning responsibilities for monitoring of data storage and security procedures and management of district data and computer and network resources, consistent with applicable internal controls.

Confidential and/or Critical Information/Data

The district will collect, create or store confidential and/or critical data/information only in accordance with state or federal law or regulations, Board policy, approved funding requirements, or when the Superintendent or designee determines it is necessary. The district will provide access to confidential and/or critical data/information to appropriately trained district employees and volunteers only when the district determines that such access is necessary for the performance of their duties. The district will disclose confidential and/or critical data/information only to authorized service providers who need access to the information to provide services to the district and who agree not to disclose the data/information to any other party except as authorized by the district and in accordance with applicable law, regulations and Board policy.

All individuals accessing or using confidential and/or critical data/information will strictly observe all administrative regulations, procedures, policies, and other protections put into place by the district including, but not limited to, maintaining hardware containing information in locked rooms or drawers, limiting access to electronic files, restricting access/use in public spaces, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information or destroying hardware no longer needed in a confidential and secure manner.

Notifications of a breach of the security of the district's computerized data system involving an individual's personal information will be conducted in accordance with law, Board policy, administrative regulations and district procedures.

Data Storage and Security Procedures

The district's data storage and security procedures will address the following:

1. The identification of the applicable industry or government standards, policies and best practices governing the proper encryption or other appropriate security measures related to transmission of data, data storage and system security that are used by the district and approved service providers.

2. Data security controls designed to protect the confidentiality, integrity and availability of information. Such data security controls may include, but not be limited to, firewalls, virus/malware detection, intrusion detection systems, encryption, and controlled software updates.

3. The appropriate monitoring of systems and platforms to assist with the prompt identification and response to misuse or breach of the security of the systems and platforms.

4. Access to district networks, platforms or computers by authorized service providers.

5. Procedures to analyze the impact of proposed program, software or platform changes prior to implementation.

6. Procedures requiring written authorization from the designated supervisor when adding, deleting or altering a user ID or access privileges.

7. Specified user password, multi-factor authentication and/or encryption requirements that meet designated industry or government standards.

8. Procedures for secure remote access of the district's network and platforms by authorized individuals.

9. Procedures for monitoring and tracking of district computers or equipment that is reported lost or stolen. Such procedures will be developed in accordance with Board policy and applicable law and regulations.

The Director of Information Technology or designee will manage all required records relating to the district's Internet, computers and network resources in accordance with auditing requirements for state and federal funding, and in compliance with applicable law and regulations, Board policy, the district's Records Management Plan and the Records Retention Schedule.

Using Online Services and Applications

District staff members are encouraged to research online platforms or applications to engage students and further the district's educational mission. District employees, however, are prohibited from installing or using applications, platforms, programs or other software, or online systems/websites, that store, collect, or share confidential or critical data/information, until the Director of Information Technology or designee approves the service provider and/or the specific

application, platform, program or other software or service used. Before approving the use or purchase of any such application, platform, program, software or online service, the Director of Information Technology or designee shall verify that it meets the requirements of the law, regulations, Board policy, and district procedures and funding requirements, and that it appropriately protects confidential and critical data/information. This prior approval is required whether or not the application, platform, program, software or online service is obtained or used without charge.

Training

The Director of Information Technology or designee will provide appropriate training to employees who have access to confidential and/or critical data/information to prevent unauthorized disclosures or breaches in security. Such training shall include, but not be limited to, identification of confidential/critical data and related storage and security procedures and rules.

Service Providers

Service providers must have the capability to comply with the district's policies and procedures, and designated industry or government standards, policies and best practices governing the proper encryption and security measures related to transmission of data, data storage and system security. An initial evaluation of the service provider's capabilities will be conducted by the Director of Information Technology or designee prior to approval of a contract or agreement with the service provider. Subsequent, periodic evaluations and monitoring will be conducted to assess service provider compliance and to identify potential risks.

Disaster Recovery Plan

The Director of Information Technology or designee will coordinate the development of a disaster recovery plan that will facilitate the actions to be taken in the event of a network security or data breach, network or server failure, or other major event which affects the district's data storage systems, computers and network resources.

The disaster recovery plan will address elements including, but not limited to, restoration of critical functions, communication to staff, integrity of confidential data, access to public records, replacement of equipment, breach notifications and resources necessary for recovery.

