Protecting your information is an ongoing, regular, and evolving process. There is no easy button, product, or single task that will make you safe from every attack. A good information security program encompasses many activities that are performed on a regular basis that work together to protect your valuable data. These 10 processes will help you get your security program started.

1. Adopt Security Framework

Acceptable security frameworks include (As defined by SB220)
NIST – SP 800-53 & 53A [LINK]
NIST – SP 800-171 [LINK]
NIST Cyber Security Framework [LINK]
Federal Risk and Authorization Management Program (FedRAMP) [LINK]
Center for Internet security controls for effective cyber defense
ISO- 27000 family of controls

2. Initial Assessment

Conduct an assessment of the School District's security program and its alignment with the selected framework. See Resource Library

3. Security Awareness Training

a. Training modules – Should be delivered to all personnel annually at a minimum and include Data Protection, Incident Identification, and Insider Threat
b. Phishing campaigns

4. Asset Inventory

Complete an inventory of information systems on network, to include workstations and servers, software, IP cameras, smart boards, other information appliances.

5. Account Management

a. Multi Factor Authentication for VPN, Administrative, and Cloud Services

b. Strong passwords (min character length, complexity requirements, reuse limits)
c. Password age – minimum 1 day and maximum 365 days.
d. Least privilege – Separate accounts for system administration and least access required to perform job duties
e. Remove inactive/unneeded accounts

6. Patching & Updates

Monthly at a minimum, review all systems on inventory, apply patches or update firmware. Apply any identified vulnerability remediation.

7. Backups

Including multiple copies, including off site

8. Endpoint Protection

Run a centrally managed anti-virus solution or EDR on all endpoints with daily updates.

9. Vulnerability Scanning

Begin utilizing DHS scanning through ITCs.

10. Incident Response, Business Continuity Planning, and Disaster Recovery

Plans should be documented and tested annually. All personnel with responsibilities within the plans should participate in the test for training. See already developed templates.

a. Incident Response Plan defines the actions and activities that are taken by the Incident Response Team in the event of a security incident or breach.
b. Business Continuity Plan defines the resumption of business processes in other than normal conditions.
c. Disaster Recovery Plan defines the resumption of IT services in support of the Business Continuity Plan.