7.16—INFORMATION TECHNOLOGY SECURITY

The superintendent shall be responsible for ensuring the district has the necessary components in place to meet the district's needs and the state's requirements for information technology (IT) security. To aid the superintendent in creating, monitoring, and updating the District's IT Security system, the superintendent shall appoint an information security officer (ISO). The ISO shall be responsible for:

a) Overseeing the District-wide IT security system;
b) Development of District IT policies and procedures;
c) Development and leading of employee training on the IT Security requirements;
d) Ensuring compliance with the adherence to the Division of Elementary and Secondary Education DESE IT Security standards

The ISO shall work with other IT staff, the superintendent, and district management appointed by the superintendent to develop a District IT Security system necessary to meet the requirements of this policy and DESE's standards. The IT security system shall contain the necessary components designed to accomplish the following:

1. The District IT security system shall contain mechanisms, policies, procedures, and technologies necessary to prevent disclosure, modification, or denial of sensitive information.

For the purposes of the IT Security system, "sensitive data" is any and all student and employee data that is either personally identifiable information (PII) or any non PII information that, if assembled together, would allow a reasonable person to identify an individual. Sensitive data includes, but is not limited to:

- Student personally identifiable information, except as allowed by the Family Educational Rights and Privacy Act (FERPA); and
- Employee personally identifiable information, except as required by Ark. Code Ann. § 6-11-129.

All District employees having access to sensitive information shall receive annual IT security training, which shall emphasize the employee's personal responsibility for protecting student and employee information.

2. Physical access to computer facilities, data rooms, systems, networks and data will be limited to those authorized personnel who require access to perform assigned duties.

User workstations shall not be left unattended when logged into sensitive systems or data that includes student or employee information. Workstation settings shall be set for automatic log off and require a password for the system to restore from screensavers.

All equipment that contains sensitive information shall be secured to deter theft. No sensitive data shall be retained on laptops and/or remote devices (home computer, thumbdrives, cell phones, CDs, etc.) unless it is encrypted in accordance with the Arkansas State Security Office's Best Practices.

Server rooms and telecommunication rooms/closets shall be protected by appropriate access control. The rooms shall be segregated from general school or District office areas to restrict access. Server room

access control shall be enforced using Keys to allow unescorted access only to IT or management staff who require the access to perform their job functions.

3. Network perimeter controls will be implemented to regulate traffic moving between trusted internal (District) resources and external, untrusted (internet) entities. All network transmission of sensitive data shall enforce encryption where technologically feasible.

The District shall maintain a network configuration management program that includes at a minimum:

a) A network diagram identifying all connections, addresses, and purpose of each connection including management approval of all high risk internet facing ports such as mail (SMTP/25), file transport protocol (FTP/20-21), etc.
b) All public facing (internet) servers and workstations segmented on a demilitarized zone (DMZ) that keeps them separate from the internal District network. Segmentation shall be through the use of routers, firewalls, and VLANS.

All wireless access shall require authentication. The DISTRICT wireless networks will deploy network authentication and encryption in compliance with the Arkansas State Security Office's Best Practices. Scans for rogue wireless devices will be conducted at a minimum monthly. Any Rogue wireless device shall be disabled.

Remote access with connectivity to the District internal network shall be achieved using encryption.

Appropriate WARNING BANNERS shall be implemented for all access points to the District internal network.

4. System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

The District shall enforce strong password management for:

- Employees and contractors as specified in Arkansas State Security Office Password Management Standard.
- Students as specified in Arkansas State Security Office K-12 Student Password Management Best Practice.

User access shall be limited to only those specific access requirements necessary for an employee to perform his/her job functions. Where possible, segregation of duties shall be utilized to control authorization access.

User access shall be granted and terminated upon timely receipt of a documented access request/termination. All access requests shall require approval by the ISO or designee. Ongoing access shall be reviewed for all users at a minimum annually.

Audit and log files shall be generated and maintained for at least ninety (90) days for all critical security-relevant events, including but not limited to:

- Invalid logon attempts;

- Changes to the security policy/procedures; and
- Failed attempts to access objects by unauthorized users.

IT administrator privileges for operating system(s), database(s), and applications shall be limited to the minimum number of staff required to perform these sensitive duties.

5. Application development and maintenance for in-house developed student or financial applications will adhere to industry processes for segregating programs and deploying software only after appropriate testing and management approvals.

Any custom-built student or financial applications or supporting applications that interface, integrate with, or provide queries and reporting to/from student or financial systems shall be developed using a system development life cycle approach that incorporates at a minimum:

a) Planning, requirements, and design;
b) User acceptance testing (UAT);
c) Code reviews; and
d) Controlled migration to production.

Any changes to core or supporting applications that provide student or financial processing or reporting shall be implemented in a controlled manner that includes at a minimum:

- Documentation of any change, including changes to both infrastructure and application;
- Management approval of all changes; and
- Controlled migration to production, including testing as appropriate.

6. Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

The District shall develop and maintain an incident response plan to be used in the event of system compromise that shall include:

a) Emergency contacts;
b) Incident containment procedures; and
c) Incident response and escalation procedures.

7. To ensure continuous critical IT services, the District ISO will develop a business continuity/disaster recovery plan appropriate for the size and complexity of the District IT operations.

The district-wide business continuity plan shall include at a minimum:

- Procedures for performing routine backups at least weekly and the storage of backup media at a secured location other than the server room or adjacent facilities. Backup media shall be stored off-site a reasonably safe distance from the primary server room and retained in a fire resistant receptacle.

- A secondary backup processing location, such as another School or District building, shall be identified.
- A documented calling tree with emergency actions to include:
  - Recovery of backup data;
  - Restoration of processing at the secondary location; and
  - Generation of student and employee listings to ensure an accurate head count.

8. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

Spyware and virus protection software shall be installed, distributed, and maintained on all production platforms, including:

a) File/print servers;
b) Workstations;
c) Email servers;
d) Web servers; and
e) Application and database servers.

Malicious software protection shall include:

- Weekly update downloads;
- Weekly scanning;
- The malicious software protection to be in active state (realtime) on all operating servers/workstations.

All security-relevant software patches shall be applied within thirty (30) days and critical patches shall be applied as soon as possible.

Legal Reference: Commissioner's Memo RT 09-010
A.C.A. § 4-110-101 et seq.

Date Adopted: 06/08/09
Last Revised: 07/08/2019