IT Security Policy (ITSP-1)	**SECURITY MANAGEMENT**

1A. Policy Statement

District management and IT staff will plan, deploy and monitor IT security mechanisms, policies, procedures, and technologies necessary to prevent disclosure, modification or denial of sensitive information.

1B. Standards

1B1 SECURITY RESPONSIBILITY

- **DISTRICTS** shall appoint, in writing, an IT Security Officer (ISO) responsible for overseeing District-wide IT security, to include development of District policies and adherence to the State-wide (ADE) standards defined in this document.

- **DISTRICTS** shall ensure that the job description and annual performance evaluation for the appointed ISO identifies IT security responsibilities.

1B2 DATA SENSITIVITY

- **DISTRICTS** shall recognize that "sensitive data" identified within this Standard is considered any and all student and employee data which is considered personally identifiable information (PII) or any non PII information which 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 (20 U.S.C. § 1232g; 34 CFR Part 99).
  - Employee personally identifiable information, except as required by Ark. Code Ann. § 6-11-129.

1B3 TRAINING

DISTRICTS, led by the Information Security Officer (ISO), shall ensure that all District employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information.

IT Security Policy (ITSP-2)	**PHYSICAL SECURITY**

2A. Policy Statement

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.

2B. Standards

2B1 WORKSTATION SECURITY

- **DISTRICTS** shall ensure that user workstations must not be left unattended when logged into sensitive systems or data including student or employee information. Automatic log off and password screen savers must be deployed to enforce this requirement.

- **DISTRICTS** shall ensure that all equipment that contains sensitive information will be secured to deter theft. No sensitive data shall be retained on laptop and/or remote devices (home computer, thumbdrives, personal digital assistances, cellphones, CDs, etc.) unless encrypted in accordance with the Arkansas State Security Office's Best Practices.

2B2 COMPUTER ROOM SECURITY

- **DISTRICTS** shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or District office areas. Server room access control should be enforced using keys, electronic card readers, or similar method with only those IT or management staff having access necessary to perform their job functions allowed unescorted access.

IT Security Policy (ITSP-3)	**NETWORK SECURITY**

3A. Policy Statement

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 should enforce encryption where technologically feasible.

3B. Standards

3B1 PERIMETER SECURITY

- **DISTRICTS** shall maintain a network configuration management program which includes as a minimum: 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.

- **DISTRICTS** using non-State supplied internet connections shall ensure that all public facing (internet) servers and workstations must be segmented on a demilitarized zone (DMZ) separate from the internal District network. Segmentation may be achieved via firewall, router, virtual local area network (VLAN), or similar network access control device which does not allow internet traffic to access any internal system without first passing through a DMZ or network device rule set.

3B2 WIRELESS NETWORKS

- **DISTRICTS** shall ensure all wireless access shall require authentication and Service Set Identifiers (SSID) shall not contain information relative to the District, location, mission, or name.

- **DISTRICTS** shall ensure that wireless networks will deploy network authentication and encryption in compliance with the Arkansas State Security Office's Best Practices.

- **DISTRICTS** shall scan for (and disable) rogue wireless devices at a minimum quarterly.

3B3 REMOTE ACCESS

- **DISTRICTS** shall ensure that any remote access with connectivity to the District internal network is achieved using encryption (e.g., SSH, RDP/High, VPN).

3B4 WARNING BANNERS

- **DISTRICTS** shall ensure that appropriate WARNING BANNERS have been implemented for all access points to the District internal network.

IT Security Policy (ITSP-4)	**ACCESS CONTROL**

4A. Policy Statement

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.

4B. Standards

4B1 SYSTEM ACCESS CONTROLS – AUTHENTICATION

- **DISTRICTS** shall enforce strong password management for employees and contractors as specified in Arkansas State Security Office Password Management Standard.

- **DISTRICTS** shall enforce strong password management for students as specified in Arkansas State Security Office K-12 Student Password Management Best Practice.

4B2 SYSTEM ACCESS CONTROLS – AUTHORIZATION

- **DISTRICTS** shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

- **DISTRICTS** shall ensure that user access should be granted and terminated upon timely receipt, and management's approval, of a documented access request/termination. Ongoing access shall be reviewed for all users as a minimum annually.

4B3 SYSTEM ACCESS CONTROLS – ACCOUNTING

- **DISTRICTS** shall ensure that audit and log files are generated and maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/configuration, and failed attempts to access objects by unauthorized users, etc.

4B4 ADMINISTRATIVE ACCESS CONTROLS

- **DISTRICTS** shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

IT Security Policy (ITSP-5)	**APPLICATION DEVELOPMENT & MAINTENANCE**

5A. Policy Statement

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.

5B. Standards

5B1 SYSTEMS DEVELOPMENT

- **DISTRICTS** shall ensure that any custom-built student or financial applications or supporting applications which interface, integrate with, or provide queries and reporting to/from student or financial systems are developed using a system development life cycle approach which incorporates as a minimum:
  - ✓ Planning, requirements, and design.
  - ✓ User acceptance testing (UAT).
  - ✓ Code reviews.
  - ✓ Controlled migration to production.

5B2 SYSTEMS MAINTENANCE AND CHANGE CONTROL

- **DISTRICTS** shall ensure that any changes to core or supporting applications which provide student or financial processing or reporting are implemented in a controlled manner which includes as a minimum:
  - ✓ Mechanisms which serve to document each change, both infrastructure and/or application.
  - ✓ Management approval of all changes.
  - ✓ Controlled migration to production, including testing as appropriate.

IT Security Policy (ITSP-6)	**INCIDENT MANAGEMENT**

6A. Policy Statement

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.

6B. Standards

6B1 INCIDENT RESPONSE PLAN

- **DISTRICTS** shall develop and maintain an incident response plan to be used in the event of system compromise which should include:
  - ✓ Emergency contacts (i.e. vendors, DIS, ADE/APSCN, law enforcement, employees, etc.).
  - ✓ Incident containment procedures.
  - ✓ Incident response and escalation procedures.

.

IT Security Policy (ITSP-7)	**BUSINESS CONTINUITY**

7A. Policy Statement

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

7B. Standards

7B1 BUSINESS CONTINUITY PLANNING

- **DISTRICTS** shall develop and deploy a district-wide business continuity plan which should include as a minimum:
  - ✓ Backup Data: Procedures for performing routine backups (as a minimum weekly) and storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room and retained in a fire resistant receptacle.
  - ✓ Secondary Location: Identify a backup processing location, such as another School or District building.
  - ✓ Emergency Procedures: Document a 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 for ensuring a full head count of all.

IT Security Policy (ITSP-8)	**MALICIOUS SOFTWARE**

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

8B1 MALICIOUS SOFTWARE

- **DISTRICTS** shall install, distribute, and maintain spyware and virus protection software on all production platforms, including: file/print servers, workstations, email servers, web servers, application, and database servers.

- **DISTRICTS** shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (realtime) on all operating servers/workstations. Districts should consider implementing enterprise servers for required updates to conserve network resources.

- **DISTRICTS** shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.