Information Technology Security Policy

Smackover School District
April 2009

(ITSP-1) Security Management

The Smackover School District Board of Directors shall appoint an IT Security Officer (ISO) who will be responsible for overseeing District-wide IT security, the development of District policies and ensuring the adherence to the State-wide Arkansas Department of Education technology standards.

The Smackover School District (hereafter called the District) shall have in place a job description for the IT Security Officer and an evaluation tool to ensure that they are following the necessary procedures to prevent disclosure, the modification of or the denial of sensitive information.

The District recognizes that "sensitive data" identified within this IT Security Policy 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. Such examples of sensitive data include, but are not limited to:

- Student or parent name, address, telephone number, and social security number;
- Student grade, attendance, medical, or transcript information;
- Student or parent financial aid or similar financial information;
- Employee name, address, telephone number;
- Employee payroll and benefits information;
- Any information which by itself or if combined with other information would lead a reasonable person to be able to discretely identify an individual.

The District, with input 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. New teachers and employees to the district may be required to receive extra training in IT security to learn the system operation and district procedures.

(ITSP-2) Physical Security

The District shall make sure that user workstations will not be left unattended when logged into sensitive systems or data including student or employee information. This will be accomplished by having automatic log off and password screen savers that will be deployed to enforce this security measure.

The District shall ensure that all equipment that contains sensitive information will be secured to discourage theft of property. No sensitive data shall be retained on laptop and/or remote devices (home computer, thumb drives, personal digital assistances, cell phones, CD's, etc) unless encrypted in accordance with Arkansas State Security Office's Best Practices. Employees are

never to use USB thumb drives, USB flash drives/flash keys, USB memory sticks, etc with any school computer. Such use of these type devices on school computers is prohibited.

The District shall ensure that rooms where servers are located and telecommunication rooms/closets are protected by appropriate access control which will segregate and restrict access from the general school or District office areas. Such rooms shall have secured access enforced by the use of 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.

(ITSP-3) Security Management

The District shall maintain a network configuration management program which includes as a minimum a network diagram identifying:

- All connections;
- All addresses;
- The purpose of each connection including management approval of all high risk internet facing ports such as main (SMTP/25), file transport protocol (FTP/20-21), etc.

The District shall ensure that all public facing (internet) servers and workstations that are non-State supplied internet connections, be segmented on a demilitarized zone (DMZ) that is 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.

The District shall ensure that all wireless access require authentication and Service Set Identifiers (SSID) that shall not contain information relative to the District, location, mission, or name. The District shall ensure that wireless networks deploy network authentication and encryption in compliance with the Arkansas State Security Office's Best Practices. The District shall scan for and disable rogue wireless devices at a minimum of each quarter.

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

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

(ITSP-4) Access Control

The District shall enforce strong password management for employees and contractors as specified in Arkansas State Security Office Password management Standard:

- At a minimum, passwords shall be changed every 90 days;
- Passwords shall be at least eight characters in length and be a mixture of alpha

and non-alpha characters;
- User passwords shall not be reused within six password changes.

The District shall enforce strong password management for students as specified in Arkansas State Security Office K-12 Student Password Management Best Practice:

- At least eight characters in length with a mixture of alpha and non-alpha Characters;
- Changed a minimum of every semester.

The District 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;
- Failed attempts to access objects by unauthorized users.

The District 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.

The District shall ensure that user access should be granted and terminated within 48 hours of the receipt, and management's approval, of a documented access request/termination. Access will be terminated as soon as possible after the last day of user employment with the District. The user will have 48 hours after employment terminates with the District to make a written request to the District for a copy of any personal data on the users District owned computer. The District reserves the right to refuse to copy any material deemed inappropriate.

The District shall limit IT administrator privileges (operating system, database, and applications) to the Information Security Officer. Any additional personnel receiving administrator privileges must be approved by the Information Security Officer and the Superintendent.

(ITSP-5) Application Development & Maintenance

This particular section of the Information Technology Security Policy does not apply to the District as the District currently utilizes the APSCN reporting system which is maintained by the Arkansas Department of Education.

(ITSP-6) Incident Management

The District shall maintain an incident response plan to be used in the event of system compromise which will include:

- Emergency contacts (i.e. vendors, DIS, ADE/APSCN, law enforcement employees, etc.);
- Incident containment procedures;

- Incident response and escalation procedures.

(ITSP-7) Business Continuity

The District shall develop and deploy a district-wide business continuity plan that will 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.

(ITSP-8) Malicious Software

The District shall install, distribute, and maintain spyware protection software (Spybot, Adware, C-Cleaner, etc.) and virus protection software (AVG., Norton, etc.) on all production platforms, including: file / print servers, workstations, email servers, web servers, application, and database servers.

The District shall ensure that malicious software protection will include frequent update downloads (minimum on a weekly basis), frequent scanning (minimum on a weekly basis), and that malicious software protection is in active state (realtime) on all operating servers / workstations.

- All personnel, classified and certified, and students will be educated in the importance of virus and spyware protection and Smackover school implementation policy.

The District shall ensure that all security-relevant software patches (workstations and servers) are applied within 30 days and critical patches shall be applied as soon as possible.