IT Security Plan Template

The attached template has numerous areas that will need to have your District information included. These areas are highlighted for your convenience in locating them within the document. It is not intended to be a final version as the District customization is extremely important to the plan.

For Information on the attached template
Please contact:

Kay Tepera or Harry Dickens
Associate Directors of Technology
Arkansas Public School Resource Center
1401 W. Capitol, Suite 465
Little Rock, AR 72201
Phone: 501-492-4300
Fax: 501-492-4305

*NOTE: This template was built collaboratively between APSRC and the coops using the State Coop technology coordinators' boilerplate for security management as a resource for developing this template. For additional assistance with this template, please contact APSRC.

IT SECURITY MANAGEMENT PLAN TEMPLATE

SECURITY MANAGEMENT

1B1 - IT Security Officer

policies and adherence to the Arkansas Department of Education state-wide standards defined in the IT Security Policy. The District has appointed _____(name of person)_____ as the IT Security for Officer for the District.

The job description for the District IT Security Officer is: (insert job description)

Example:

ISO Job description

- Administrative authority to enforce district IT security policies
- Develop District IT policies
- Enforce adherence to local and State-wide (ADE) standards (defined in the state policy standards document)
- Insure that employees have appropriate annual security training emphasizing their personal responsibility to protect sensitive information
- Work with school district technical staff, state and coop resources to maintain compliance with best practices in IT security and keep abreast of latest security and privacy legislation, regulations, advisories, alerts and vulnerabilities.
- Ensure that the district adheres to FERPA, CIPA and HIPPA standards in protection of sensitive data
- Take part in District Recovery Planning.

An annual performance evaluation of the ISO is conducted and maintained on file at the District's Central Office.

1B2 – Data Sensitivity

The District recognizes that sensitive data is considered to be any and all student and employee data which is 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 allow 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

The District ensures 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. A copy of this training will be kept on file at the District Central Office.

PHYSICAL SECURITY

2B1 – Workstation Security

groups. The following is a list of user groups and the customized wait time that has been assigned per group. [The District might consider using a technology committee to determine appropriate groups and wait time per group. Use this list as an example and customize to fit the needs of your district.]

- Administrators
- IT Technology
- Teachers
- Support Staff

(Recommended 15 minutes or less for non-presentation devices).

The District will train employees on the method to lock workstation if leaving the computer. (CTRL, ALT, DEL if on a domain, or using the Windows Key L if stand alone, or applicable to the computer)

The District will use (See coop tech coordinators comments at end of document for recommended programs) to encrypt data on all removable devices such as laptops and USB drives that contain sensitive data. The District will stress to employees that downloads of data from TRIAND, APSCN, D2SC, NORMES, etc., constitutes sensitive data. The District will not allow staff to download data to home computers unless it is encrypted.

2B2 – Computer Room Security

The District shall ensure security of server rooms and telecommunication closets by using locked doors with (Choose: key, electronic card or other method) that restricts access. The District ISO will work to ensure that only IT or management staff in the fulfillment of duties, are allowed access to the above mentioned rooms.

NETWORK SECURITY

3B1 – Perimeter Security

firewall.

The District will [choose one 1. Use the state provided firewall through the router 2. A self maintained firewall (ex: SonicWall, IPCop, Bordermanager, ISA Server)] to protect the local network from outside attacks.

The District will not implement non-state provided internet access unless capable of creating a DMZ or Virtual Local Area Network to segment the traffic and deny internet access from the external system into the internal (state) network. [For districts desiring to increase bandwidth through external internet access, please see coop tech coordinators comments at end for options that could be used.]

3B2 – Wireless Networks

The District has changed the SSID for wireless using a naming convention that does NOT indicate the purpose, location or District information:

The coop tech coordinators suggest this possible add on statement: [The District will turn off SSID broadcast on access points as often as possible realizing that guests may need access to certain access points for presentation and internet access.]

The District will change all default access point management passwords.

The District will use [pick the strongest available that you are using WPA, WPA2, Other] encryption and authentication method on wireless access points. The District will change shared encryption keys every 30 days and keep a record of the date the change was made.

The District will scan, disable if found, and keep a record of the scans for rogue wireless devices on a quarterly basis (at a minimum).

3B3 – Remote Access

The District will use [choose one or more: 1. SSH, 2. RDP, 3. VPN 4. name of other] for any remote access connections to the internal network from a hot spot or home connection. [Note VPN and RDP are free and supported by Windows, VPN and SSH are free supported on Linux, VNC with encryption is supported on multiple systems]

3B4 – Warning Banners

The District will implement login banners stating acceptable use policy or location of stated policy which by logging in is accepted by the user. (Check the Tools4Techs web site for instructions and examples).

The District's warning banner displays: (insert the words here)

ACCESS CONTROL

4B1 – System Access Controls: Password Management

[x (min 8)] characters in length with a mix of alpha and non-alpha, and not reused within [x (min 6] times. To ensure accountability employee passwords must be private and users can be held responsible for the security of their passwords. School administrators and technical staff should not keep a list of employee passwords but those with administrator rights to the system may access accounts by changing the user's password as required.

The District will adhere to the State Security Office K-12 Student Password Management Standards. Students in grades K – 3 will use the following procedure for access to the system and computers: [Enter your procedure here]

Students in 4-12 require a password with [x (min 8] characters in length with a mixture of alpha and non-alpha characters, and changed every semester. Students with elevated privileges [list reasons here ex: student network assistant ex: EAST lab students] will follow the employee management standard.

4B2/4B4 – System Access Controls: Authorization & Access Controls

The District will limit access to data, programs and networks to the minimum necessary to perform job duties. A detailed list of user/group access will be maintained by the ISO.

The District will grant and revoke access in a timely manner. A sample form used to document the requests indicating management approval can be found in the site notebook. The technology department will work with the school administration to review access on at least a yearly basis. The site notebook will contain a list of programs, web application and network access that should be reviewed in this process.

The District will limit administrator privilege to the minimum staff to perform the duties. The site notebook will contain a detailed list of administrative users and their access rights.

4B3 - Accounting

The District will configure servers to maintain logs dealing with security relevant events.

APPLICATION DEVELOPMENT & MAINTENANCE

5B1 – Systems Development, Maintenance and Change Control

Changes or upgrades to in house or custom designed programs that interface with Pentamation/APSCN shall be implemented in a controlled manner commonly known as change management procedures.

INCIDENT MANAGEMENT

6B1 – Incident Response Plan

- Emergency Contacts
- Incident containment procedures
- Incident response and escalation procedures

This information can be obtained _____

BUSINESS CONTINUITY

7B1 – Business Continuity Plan

The District will develop criteria that identify critical data requiring electronic backup and a list of those criteria and the data involved and will be included in the site notebook. Procedures for backing up the data will also be developed and included in the site notebook.

The District will use [enter back up processing location with approved MOU] as a backup processing location.

It is recommended to include IT business continuity in the schools total business continuity plan using software such as the state's Continuity of Operations Plan (COOP) program.

MALICIOUS SOFTWARE

8B1 – Malicious Software

workstations, web servers, and database servers.

The District will base its selection of anti-virus and anti-spyware software on the ability to schedule updates at least weekly, schedule scanning at least weekly, run in an active (real-time) state and the capability of the software to protect the systems. [Recommended that the products be capable of using local resources for updates]

The District will use [choose one 1. Automatic updates directly from Microsoft or other OS vendor 2. WSUS managed updates] to ensure that patches are applied within 30 days or sooner for critical patches.

****Notes, thoughts, and suggestions on IT security policy by the Coop Tech Coordinators**

1B1:

Recommendation is that the I.S.O. not be a district technician or system administrator due to possible conflicts of interest. Additionally, this position should be filled by someone with administrative authority who can discipline personnel and students who violate policy.

As an alternative, it was suggested that the I.S.O. be the person in charge of "reporting" policy violations and the discipline be then handled at the administrative level.

1B2:

Nothing to add, this updated language simply keeps us in line with F.E.R.P.A. as it has been modified to cite the specific state and federal laws that it was originally intended to support.

1B3:

ALL employees could potentially have access to sensitive data. Because of this, districts should think broad-mindedly as they decide who should undergo annual IT Security training. As pointed out in the policy, this training emphasizes employees' personal responsibility for protecting student and employee information.

There are no current recommendations by the state in regards to how much time this training should be provided for. The state Co-op technology coordinators feel this training could be realistically obtained in one hour.

It was mentioned that this type of training should be provided and placed on I.D.E.A.S. portal.

2B1:

Recommendation to change the wording of 2B1 due to the fact that Automatic log off AND password screen savers could be technically redundant. IF the intent was for automatic log off to apply to any applications provided by the district and for screen saver passwords to be implemented on workstations then the policy/procedure should be modified to be more specific.

At this time, we recommend that password protected screensavers be implemented on workstations and that automatic time-limited log off of district supplied applications be enforced.

The time limit should be determined by the district's I.S.O, under the advisement of the district's tech committee. (Or if they would just change "and" to "or" it would make more sense.)

A potential conflict exists as portable access becomes more and more readily available and expected. Employees increasingly access data from private equipment that is not owned or supplied by districts. Because of this, districts should consider developing a policy that should be signed off on after the annual training required in 1B3 to ensure that employees will not retain sensitive data on personal, privately owned devices, included but not limited to mobile phones, portable storage devices, and home computers.

School-owned portable devices will have to be encrypted, if sensitive data is to be accessed, in order to be in compliance. There are commercially available software encryption products available, as well as no up-front cost open source products that provide this encryption.

In a best-effort against inadvertent retention due to web-page caching of information, it is suggested that a minimal amount of drive space and time be allocated for workstation web-page caching.

Enterprise encryption currently available and evaluated by co-ops:

Guardian Edge	$35 for hard drive and removable storage - perpetual license
McAfee	$13 for hard drive, $35 for hard drive and removable storage 3-year
Sophos	$22 for hard drive and removable storage - 18 months
DeepFreeze	could potentially be used as a solution for this ~$35 per machine in small

quantity and can be perpetual.

Open-Source or no-cost

True-Crypt

Built-in Windows or MAC OS encryption (limited to folders only)

SteadyState by Microsoft

2B2:

New wording that specifies server room makes this easier for us to live with.

Put a lock on the door to the server closet.

3B1:

District tech personnel will maintain accurate and updated site notebooks.

Microsoft Visio, D.I.A., and network notepad are all products that will aid in the creation of network diagrams.

D.I.S. also provides assistance in creation of site notebooks.

Part 2 of this only affects districts and campuses that have obtained 3rd-party internet connectivity other than that which is available from the State-supplied DIS connections.

3B2:

Rogue scanning should not only take place, but records should be kept to document the frequency and results of the scans.

Net stumbler is a free and open-source software application that can aid in the discovery of rogue wireless network.

3B3:

3B4:

Warning banners can be implemented using login scripts. Look on Tools4techs website for examples.

4B1:

Employee passwords will have to be 8 characters, mixture of alpha and numeric characters, must be changed every 90 days, and cannot be repeated for 6 periods.

Student passwords (4^{th} grade and older) will have to be 8 characters, mixture of alpha and

numeric characters, must be changed every semester, and cannot be repeated for 6 periods.

4B2:

Administration, Human Resources, and Counselors must keep IT Director informed of personnel and student status changes. Access and file/directory rights will need to be reviewed annually and student accounts must be terminated upon graduation.

Triand, APSCN, and other non-district owned systems must also be taken into consideration as these systems are often outside the scope of the district IT staff.

4B3:

Windows and Novell servers have this capability built-in.

D.I.S. is working out instructions on how to ensure this is setup and running.

5B1:

Only affects districts developing their own applications to interface with APSCN.

We feel this is NOT grade book or cafeteria programs.

6B1:

Districts will need to ensure that emergency contact information is up-to-date at DIS so that their M.A.R.S. network monitoring software can effectively contact appropriate personnel may be contacted at the district level.

7B1:

Data should be backed up from the server as suggested. Also, any data necessary for business continuity that is run from local workstation should be backed up as well.

Districts can work with the co-op or other district locations as a secondary location.

An agreement on paper should exist to document this.

Also, as a best practice, a second secondary (tertiary) location agreement should exist, outside of 25-mile proximity in the event of a geographic catastrophe.

Continuity of Operations Plan (COOP) can be referred to help comply with this.

8B1:

Anti-Spyware, malware, and anti-virus software should be maintained and kept up-to-date on all workstations.

Windows S.U.S. service and/or Apple Update service should be implemented to ensure that

operating system patches and updates are installed in a timely manner.

*NOTE: This template was built collaboratively between APSRC and the Coops using the State Coop technology coordinators' boilerplate for security management as a resource for developing this template.