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

JASPER SCHOOL DISTRICT 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. . An IT Security Officer is responsible for enforcement of policies, not technical implementation.

JASPER SCHOOL DISTRICT shall ensure that the job description and annual performance evaluation for the appointed ISO identifies IT security responsibilities.

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.

1B2 DATA SENSITIVITY

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.

Jasper School District IT Security Policies

Preamble

In compliance with the State of Arkansas Best Practices, the Arkansas Department of Education, and generally accepted industry best practices, the Jasper School District provides for the security and privacy of the data stored on, redirected through, or processed by its technology resources. The Jasper School District encourages the use of these technology resources; however they remain the property of the Jasper School District and are offered on a privilege basis only. Throughout this policy, the term "staff" identifies full- and part-time employees, contractors, consultants, temporaries, student assistants, volunteers, retired annuitants, vendors and other users including those affiliated with third parties who access Jasper School District technology resources due to their job responsibilities. Management expects staff to comply with this and other applicable Jasper School District policies, procedures, and local, state, federal, and international laws. ***Failure to abide by these conditions may result in forfeiture of the privilege to use technology resources, disciplinary action, and/or legal action.***

The IT Policy Review Team regularly modifies this and other IT security related policies to reflect changes in industry standards, legislation, technology and/or products, services, and processes at the <company>.

Privacy

The Jasper School District reserves the right to monitor, duplicate, record and/or log all staff use of Jasper School District technology resources with or without notice. This includes but is not limited to e-mail, Internet access, keystrokes, file access, logins, and/or changes to access levels. ***Staff shall have no expectation of privacy in the use of these technology resources.***

Liability

The Jasper School District makes no warranties of any kind, whether expressed or implied for the services in this policy. In addition, the Jasper School District is not responsible for any damages which staff may suffer or cause arising from or related to their use of any Jasper School District technology resources. ***Staff must recognize that Jasper School District technology resource usage is a privilege and that the policies implementing said usage are requirements that mandate adherence.***

Staff Responsibilities and Accountability

Effective information security requires staff involvement as it relates to their jobs. Staff is accountable for their actions and therefore they own any event(s) occurring under their user identification code(s). It is staff's responsibility to abide by policies and procedures of all networks and systems with which they communicate. Access of personal or private Internet Service Providers while using Jasper School District provided information technology resources or using non-Jasper School District provided information technology resources to conduct Jasper School District business does not indemnify any entity from the responsibilities, accountability and/or compliance with this or other Jasper School District policies. Staff responsibilities include but are not limited to:

- Access and release only the data for which you have authorized privileges and a need to know (including misdirected e-mail)
- Abide by and be aware of all policies and laws (local, state, federal, and international) applicable to computer system use
- Report information security violations to the Information Security Officer or designee and cooperate fully with all investigations regarding the abuse or misuse of state owned information technology resources
- Protect assigned user IDs, passwords, and other access keys from disclosure
- Secure and maintain confidential printed information, magnetic media or electronic storage mechanisms in approved storage containers when not in use and dispose of these items in accordance with Jasper School District policy
- Log off of systems (or initiate a password protected screensaver) before leaving a workstation unattended
- Use only Jasper School District acquired and licensed software
- Attend periodic information security training provided by Jasper School District IT Security Branch
- Follow all applicable procedures and policies

Electronic Mail (E-Mail) Policy

The Jasper School District electronic mail services (e-mail) policy provides staff with guidelines for permitted use of the Jasper School Districted-mail technology resource. The policy covers e-mail coming from or going to all Jasper School District owned personal computers, servers, laptops, paging systems, cellular phones, and any other resource capable of sending or receiving e-mail.

Ownership

The Jasper School District owns all e-mail systems, messages generated on or processed by e-mail systems (including backup copies), and the information they contain. Although staff members receive an individual password to access the e-mail systems, e-mail and e-mail resources remain the property of the Jasper School District.

Monitoring

The Jasper School District monitors, with or without notice, the content of e-mail for problem resolution, providing security, or investigative activities. Consistent with generally accepted business practices the Jasper School District collects statistical data about its technology resources. Jasper School District technical staff monitors the use of e-mail to ensure the ongoing availability and reliability of the systems.

Accountability

Staff may be subject to loss of e-mail privileges and/or disciplinary action if found using e-mail contrary to this policy. Staff must maintain the confidentiality of passwords and, regardless of the circumstances, ***never share or reveal them to anyone***. The Information Security Officer (ISO) must provide express written permission before sensitive information is forwarded to any party outside of the Jasper School District. Staff should contact the ISO with questions regarding the appropriateness of information sent through e-mail.

Ethical Behavior and Responsible Use

The Jasper School District provides e-mail systems to staff to facilitate business communications and assist in performing daily work activities.

Ethical and Acceptable

- Communications and information exchanges directly relating to the mission, charter, and work tasks of the Jasper School District
- Announcements of laws, procedures, hearings, policies, services, or activities

- Notifying staff of Jasper School District sanctioned employee events, such as the holiday party, bake sales, arts and craft fairs, retirement luncheons, and similar approved activities
- Respecting the legal protection provided by all applicable copyrights and licenses
- Practicing good housekeeping by deleting obsolete messages

Unethical and Unacceptable

- Violating ***any*** laws or Jasper School District policies or regulations (e.g. those prohibiting sexual harassment, incompatible activities, or discrimination)
- Submit, publish, display, or transmit any information or data that contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory, or illegal material
- Compromising the privacy of staff, customers, or data and/or using personal information maintained by the Jasper School District for private interest or advantage
- Engaging in any activities for personal gain, performing personal business transactions, or other personal matters (e.g. sending sports pool or other gambling messages, jokes, poems, limericks, or chain letters)
- Intentionally propagating, developing, or executing malicious software in any form (e.g. viruses, worms, trojans, etc.)
- Viewing, intercepting, disclosing, or assisting in viewing, intercepting, or disclosing e-mail not addressed to you
- Distributing unsolicited advertising
- Accessing non-Jasper School District e-mail systems (e.g. Hotmail, Yahoo!) using Jasper School District owned resources

Reinforces Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
    - School officials with legitimate educational interest;
    - Other schools to which a student is transferring;

Specified officials for audit or evaluation purposes;
Appropriate parties in connection with financial aid to a student;
Organizations conducting certain studies for or on behalf of the school;
Accrediting organizations;
To comply with a judicial order or lawfully issued subpoena;
Appropriate officials in cases of health and safety emergencies; and
State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For additional information or technical assistance, you may call (202) 260-3887 (voice). Individuals who use TDD may call the Federal Information Relay Service at 1-800-877-8339.

Or you may contact us at the following address:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-5920

1B. Standards

JASPER SCHOOL DISTRICT 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 or parents 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.

1B.A Risk Management

Overview of Risk Management

Overview

The purpose of this module is to familiarize employees with risk management. To do this, employees first must understand the key attributes of risk and the concepts underlying risk management (including risk analysis assessment). One of these key attributes is the valuation and determination of assets. In most organizations, this process consists of identifying and prioritizing assets based on their value, cost, or importance. This module focuses on organizations that select and prioritize assets based on the assets' importance or relevance to fulfilling the mission and objectives of the organization.

This module also introduces concepts such as risk, risk impact, risk attributes, assets, asset categories, risk analysis, and risk management. Additionally, this section examines the application of risk management. This examination includes a description of risk assessment and analysis activities, comprehension of the impact of risk events, and recognition of mitigation strategies for managing and reducing risk.

Risk

Risk is the potential that a given threat will exploit vulnerabilities of an asset and compromise its CIA.

1.B.A.1 Description of Risk

Risk is the possibility of suffering harm or loss. With respect to information and computer data, risk is the potential that a given threat will exploit vulnerabilities to compromise an asset's confidentiality, integrity, or availability.

Before risks can be managed, they must be identified. One way to identify potential risk is to list the components of risk in an asset-driven scenario and gauge the risk's plausibility.

Example of Risk
For example, let's consider a home user making a consumer purchase over the Internet. In this situation, the user must submit customer information to the Web site (i.e., item, quantity, name of customer, address of customer, payment type, credit card number, etc.) to complete the purchase. Therefore, from the user's point of view (even if he or she is not explicitly aware of the risk or is seemingly unconcerned about it), risk exists. To identify the risk in this situation, we can state that the asset is the customer's information, the threat is anyone on the Internet with malicious intent, and the vulnerability is any technology weakness that allows the information to be observed and captured.

Threats and Vulnerabilities
Probably the most readily identifiable components of risk, to system and network administrators, are threat and vulnerability. The combination of threat and vulnerability yields a potential for undesirable outcomes, as when threats exploit vulnerabilities in an asset to compromise the asset's confidentiality, integrity, and/or availability. These undesirable outcomes are referred to as impacts.

Risk Impact
Compromising CIA of critical assets can cascade into loss of

- Key technologies
- Competitive position
- Customer confidence
- Trust
- Revenue
- Life or property
- Financial stability. monetary fine, law suit, or regulatory penalty

1.B.A.2 Risk Impact
Understanding a risk's impact forms the basis for evaluating outcomes of risk: loss, destruction, modification, and interruption. Impact is the actualization of risk. To evaluate the outcome of a risk, we start by developing evaluation criteria for risk scenarios.
For example, consider a home user who sets up a personal Web server to display his or her resume. As a risk management process, our home user identifies his or her assets, considers possible negative outcomes, and characterizes the potential impact of an asset's compromise. Here, our home user recognizes that one asset is the Web server itself, while another is his or her resume. Possible negative outcomes to the resume asset include

- Destruction of the resume file
- Modification of the resume content
- Pirating of the resume data
- Interruption of the resume's presentation to the Internet

After considering these potential negative impacts, our home user should be able to define potential failure conditions, such as

- Destruction, causing an expenditure of effort to restore or recover the information
- Modification, causing a prospective employer to consider the candidate either adequate or inadequate for the position, depending on what information was changed

- Theft, causing a loss of creative and competitive marketing of the individual's skills or background
- Interruption, causing an inability for potential employers to view the candidate's information

Finally, the home user must decide whether he or she really cares about the potential impacts to his or her assets. If yes, then mitigation strategies should be supplied; if no, then the potential risk impacts are accepted in addition to the consequences of loss or harm that could be suffered through exposure to the risk.

Components of Risk

RISK Asset
Threat Vulnerability

1.B.B Components of Risk

For a risk to exist, the following must be present:

- Assets of value to an organization or individual that must be protected (critical assets)
- Threats to these critical assets (possibility of disclosure, modification, destruction, or interruption)
- Vulnerabilities of these critical assets that may provide an opportunity for threats to act on the assets in a manner that discloses, modifies, destroys, or interrupts the assets

Identifying assets involves a discussion within the organization to determine what categories of assets exist, who owns each asset, and what level of protection is necessary for each asset. This exchange of information should take place between managers, staff, and information technology personnel on a periodic basis and as part of the organization's review of its information security policy. These events are important as a means of identifying assets and risk mitigation plans because they enable the organization to identify its current protection strategy for each asset and any changes to the asset's priority. This priority discussion allows a ranking of some assets over others, and it should be documented and reflected in organizational policy, recognizing that assets may be mission critical, non-critical but sensitive, or general in nature.

Relating threats and vulnerabilities to an asset is part of risk assessment and requires that those responsible for protecting information assets have an appreciation of the range of threats and vulnerabilities. Once the range is known, the likelihood of any one threat acting adversely on an asset must be understood.

The results of risk analysis identify the strategies (plans, policies, technological mechanisms) that can help mitigate the risk. Analysis includes evaluating the risk to an organization and measuring that risk against the impact to the organization if the risk is realized. For example, a determined risk for a medical organization may be that "modification of paper medical records by unauthorized individuals can lead to loss of life, financial or punitive penalties, or loss of customer confidence." In this case, this risk is actually stated as a risk scenario that includes assets (paper medical records), threat actors (personnel exceeding their privileges or unauthorized outsiders), outcome (modification of the records), and impact (public safety, financial, customer confidence, legal). Risk analysis determines which risks are viable (that is, non-negligible) and what degree of impact (high, medium, or low) the risk has on the organization when evaluated.

1.B.C Identify Assets

An asset is anything of value to an organization. Typically, assets are classified as information assets (people, hardware, software, systems), other supporting assets (facilities, utilities, services), or critical assets. Critical assets may include information or other supporting assets. Later in this section, we will describe examples within each category.
It is important to note that your organization may choose to classify assets within different categories according to sensitivity or function. Asset definitions may be highly subjective, and asset value even more so; therefore, an easier way to approach assets and asset value can be to consider the worth of the asset (in both tangible and intangible terms) to the organization. By examining the costs associated with the value and intrinsic value of an asset (qualities of the asset's existence), you may discover a more meaningful definition and value of the asset.

Information includes

- data being processed on, stored on, or transmitted between systems
- backup and archive data (on-site and off-site storage volumes and locations)
- paper documents
- escrowed encryption keys
- software distribution media

Hardware includes

- desktop computers
- servers
- mainframes
- network equipment (routers, switches, firewalls)
- wiring infrastructure
- wireless support infrastructure

Software includes

- commercial off-the-shelf (cots) software
− operating systems
− desktop software
− mainframe applications
- custom software
− in-house effort
− outsourced effort
− ad hoc scripts
− undocumented tools used by employees

People include

- senior and middle management
- technical and non-technical staff
- public relations
- help desk, facilities, security

• contractors, third parties (Computer Security Incidence Response Teams [CSIRTs])
• government, police, fire

Facilities include
• heating/ventilation/air conditioning (hvac) support
• power
• water
• telephone
• security

Utilities include
• power
• water
• telephone
− leased lines (t1, t3, isdn)
− voice lines
− cell phones
• pager services
• service-level agreements
− hardware maintenance
− HVAC support

Outsourced services include
• off-site services
− information storage
− Web services
• consultants
• utilities
• legal services
• public relations
• managed or monitored security
− physical
− network

Identify Critical Assets

Critical Assets are assets determined to have an integral relationship with the mission of the organization and its success.

Examples:

- Intellectual property /patents / copyrights
- Corporate financial data
- Customer sales information
- Human resource information

1.B.C.1 Identify Critical Assets

Critical assets are assets that have an integral relationship with the mission of the organization. This means that loss or damage to a critical asset would cause disruption to the operational or functional mission of the organization to a point where the mission fails. This concept recognizes that each individual organization will define a different and unique set of critical assets that align with mission success or failure.

Examples of critical assets include

• intellectual property
− patents, copyrights
− software code under development
− systems acquisition or
development projects
• corporate financial data
− payroll information by employee, department, organization
− financial earnings, revenue, and loss statements
− stock dividend information
• customer sales information
− names, addresses, credit card /account numbers, purchase histories, demographic information
• human resource information
− names of employees, departments, salaries
− hiring, administrative punishment, and disability information
• network architecture information
− network topology diagrams
− desktop or systems replacement plans
− strategic infrastructure plans
− vulnerability assessment reports
− types and locations of infrastructure (general purpose, storage, server, networking, and security devices)
• U.S. Government or state government classified information
− compartmentalized projects
− deployment and strategic plans
− intelligence information, logistic movements/support
− technical specifications on equipment, weapons, projects

Identify Security Requirements

Each critical asset has different requirements of confidentiality, integrity, and availability that should be

- Documented
- Communicated

1.B.C.2 Identify Security Requirements

Each critical asset has different requirements for *confidentiality*, *integrity*, and *availability* that should be

• documented, describing the requirements, the responsible information/asset owner(s), and the party charged with the asset's protection, as well as under what conditions and to what degree the requirements must be enforced

• communicated throughout the organization, especially from the owner of the asset to the person(s) responsible for its safety and security (the information/asset custodian)
Security requirements should be understood at all levels of the organization involved in the asset's protection. They should be described with enough detail for a specific requirement to be placed on the responsible owner (manager, user, system/security administrator, etc.) or the technology protecting the asset. They should be documented in security policies and plans.

Vulnerabilities

Weaknesses in an asset

- Software Weaknesses
- Weak default settings

Default accounts/passwords, access controls, unnecessary software

- Bugs
- Buffer overflows, poor error handling
- Architecture Weaknesses
- Single points of failure
- Personnel Weaknesses
- Lack of awareness/training

1.B.C.3 Vulnerabilities

Vulnerability is the absence or weakness of a safeguard. It can also be described as a weakness in an asset or in the methods of ensuring that the asset is survivable. The examples of vulnerabilities listed on this slide provide a small sampling of the numerous classes of vulnerabilities that commonly exist.

Threats

Events that may compromise the CIA of an asset (i.e., exploitation of vulnerabilities)
Common threat tools/techniques:

- Malicious Code
- Worms, Viruses, Trojans, DoS
- Social Engineering
- Packet Sniffing and Network Scanning

1.B.C.4 Threats

A threat is any event that will cause an undesirable impact or loss to an organization if it occurs. Examples of threats include the following:
• intrusions into and disruptions of information systems
− viruses, worms, and Trojan horses
− denials of service
− sniffing network traffic
− stealing data assets
• loss of assets that are single points of failure
− critical data that is not backed up
− a single, critical piece of network infrastructure (i.e., a core router)
• keys that are used to encrypt critical data

Calculating Risk Exposure
Qualitative Risk Analysis

- Probability x Severity
- Risk Assessment Matrix

Quantitative Risk Analysis

- Potential Financial Loss

1.B.D Calculating Risk Exposure

Risk analysis is the process of identifying security risks, determining their magnitude, and identifying areas in need of safeguards. Risks are traditionally captured as a description that can then be measured both qualitatively and quantitatively. Qualifying a risk means understanding the potential negative impact with respect to the asset as well as the likelihood of the threat. This impact occurs when the asset is destroyed, modified, interrupted, or disclosed. To home users, qualifying risk often means evaluating the impact of having their personal information disclosed. In this case, the users will probably be most concerned with their financial liability, chance of identity loss, and laws and regulations to which they may be subjected, as established by a qualitative scale (or criteria) for evaluating the risk (such as high, medium, or low).

Quantifying risk means understanding the possibility of the risk existing or coming to fruition. Here the home user attempts to measure the probability or likelihood of someone performing several different attacks whose goals are to retrieve his or her personal information. This measurement takes into account how likely it is that

• someone may observe the information in transit between the home user and the Web site (and possibly decode the encrypted network traffic)
• the software making the exchange of personal information is vulnerable to attack
• the user will be singled out for exploitation over all of the other Web commerce transactions happening at the Web site of purchase
• an attacker might gain access to the information once it has arrived at the Web site

These are just a small sample of the risks involved in this simple transaction. For the individual to really understand these risks, he or she must appreciate the potential impact of these risks. This demands an understanding of the potential that threat sources (humans, system problems, viruses, etc.) have in exploiting and abusing vulnerabilities that result in risk. This potential falls into a continuum ranging from negligible to actual, over the life of the information being transmitted, stored, and processed.

Quantitative risk analysis can be a major project and can consume considerable organizational resources. It attempts to assign independently objective numeric values (hard dollars, for example) to the components of risk assessment and to the assessment of potential losses. Qualitative risk analysis addresses more intangible values of loss and typically attempts to produce scenarios so risk can be anticipated and managed. However, threat frequency and impact data is still required to conduct a qualitative risk analysis.

Use exposure values to:
. **Prioritize the order in which risks are addressed**
. **Help in deciding how to manage risks**
A new worm attacks vulnerable systems

Web site defacement
Datacenter flooded by fire protection system

Qualitative Risk Analysis

1.B.D.1 Qualitative Risk Analysis

Exposure Factor (EF)

- % of loss of an asset

Single Loss Expectancy (SLE)

- EF x Value of asset in $

Annualized Rate of Occurrence (ARO)

- A number representing frequency of occurrence of a threat. Example: 0.0 = Never 1000 = Occurs very often

Annualized Loss Expectancy (ALE)

- Dollar value derived from: SLE x ARO

3.4.2 Quantitative Risk Analysis

Managers in IT are often faced with the dilemma of justifying their expenditures on survivability and security. Ideally, resources allocated toward survivability should be seen as an investment in the mission of the organization. But because the old paradigm (security seen as an overhead expense) is still an operational reality, IT managers often justify expenditures with forms of quantitative risk analysis. The terms shown on this slide are pseudo-standards that can help calculate risk in relation to actual dollar figures. Their usage helps to provide more reliable cost-benefit analysis.

• Exposure Factor (EF)

The exposure factor describes the effects a realized threat would have on a particular asset as a percentage of loss of the total value of the asset. For example, loss of some hardware would have a small EF, whereas the catastrophic loss of all computing resources would have a large EF. The EF value is necessary to compute the Single Loss Expectancy (SLE), which in turn is necessary to compute the Annualized Loss Expectancy (ALE).

• Single Loss Expectancy (SLE)

The single loss expectancy is the dollar figure assigned to an organization's loss from a single threat event. It is derived from the formula EF X asset value in dollars = SLE. For example, an asset valued at $10,000 that is subjected to an EF of 50 percent would yield an SLE of $5,000.

• Annualized Rate of Occurrence (ARO)

The annualized rate of occurrence is a number that represents the estimated frequency with which a threat is expected to occur. This value can range from 0.0 (for threats that never occur) to a large number (for threats that occur frequently, such as misspellings of names in data entry). This number is usually created based on the likelihood that the threat will occur and the number of individuals that could cause it to occur. The loss incurred by this event is not a concern here, only how often it occurs.

• Annualized Loss Expectancy (ALE)

Annualized loss expectancy (ALE) is the annual financial loss an organization expects from a threat. It is calculated by multiplying the single loss expectancy and annualized rate of occurrence (SLE X ARO = ALE). For example, a threat with a dollar value of

$10,000 (SLE) that is expected to occur 5 times per year (ARO) will result in an ALE of $50,000 [Krutz 2001].

Generally speaking, if an organization's information survivability expenditures are less than the sum of the calculated ALEs, than some quantitative return on investment (ROI) figures can be discerned.

Summary of the Assessment Step

Risk is the probability and severity of loss from exposure to a threat. The assessment step involves the application of quantitative or qualitative measures to determine the level of risk associated with a specific threat. Specifically, this process evaluates the probability and severity of an undesirable event that could result from the threat.

Risk Management

Process of assessing and quantifying risk and establishing an acceptable level of risk for the organization

Risk can be mitigated, but cannot be eliminated.

1.B.E Risk Management

Risk management should be a well-defined and established process. Effective risk management can save resources, reduce mishaps, and even save lives.

Managing Risks

Acknowledge that the risk exists, but apply no safeguard (Exposure value is within tolerance)
Shift responsibility for the risk to a third party (ISP, MSSP, Insurance, etc.)
Change the asset.s risk exposure (apply safeguard) Eliminate the assets exposure to risk, or eliminate the asset altogether.

1.B.E.1 Risk Management Strategies

Organizations have four options when deciding how to manage risks:

1. Accept

If an organization chooses to accept risk, it does so with full knowledge of the potential threats and vulnerabilities to the asset. It may be that the asset's exposure is acceptable or within some level tolerance. For example, an organization recognizes the threat that usernames and passwords could be compromised by administering systems remotely with telnet, a protocol that transmits data, including passwords, in plaintext. However, the organization decides the risk is not great enough to warrant a safeguard (i.e., encrypted sessions with SSH or IPSec).

2. Mitigate

Mitigating risk is the process of actively applying safeguards to reduce an asset's level of exposure. In the above telnet example, the organization could mitigate the risk by (a) denying all management traffic to the remote systems that is not encrypted and authenticated, and (b) writing an organizational policy that acts as a deterrent (i.e., any attempt to compromise access controls on organizational systems will be met with stiff disciplinary action).

3. Transfer

Transfer of risk occurs when an organization decides to contract with a third party to mitigate the risk. For example, an organization can transfer the risk of losing data (and support the goal of mission survivability) by contracting with a service provider that maintains an off-site data backup and recovery capability. Although risk transference does not change the probability or severity of a threat, it may decrease the probability or severity of the organization's risk. At a minimum, the organization's risk is greatly decreased or eliminated because the possible losses or costs are shifted to another entity.

4. Avoid

Avoiding risk means that the organization eliminates the asset's exposure or even the asset itself. An example might be the replacement of historically vulnerable platforms (like Internet Information Server) with hardened platforms like a Bastille/Apache Web server solution [Bastille 06].3F

4 See http://www.bastille-linux.org/.

Summary

Risk

- The possibility of compromising an asset.s CIA
- Composed of assets, threats, and vulnerabilities
- Exposure measurement may be qualitative or quantitative
- May be avoided, accepted, mitigated, or transferred
- Can be mitigated, but never eliminated

1.B.F Summary

Sustaining and improving information security is a continuous risk management activity.

Risk is comprised of assets (something of value to the organization), threats (concerns related to undesirable outcomes), safeguards, and vulnerabilities (weaknesses creating the possibility for threats to negatively impact the organization).

Risk analysis, a major component of risk assessment, helps to identify the possibility of certain risks and the impact when risks are realized. Because information cannot be realistically managed to have no risk, at some point risk must be accepted.

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.

1B2 DATA SENSITIVITY

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.

Jasper School District IT Security Policies

Preamble
In compliance with the State of Arkansas Best Practices, the Arkansas Department of Education, and generally accepted industry best practices, the Jasper School District provides for the security and privacy of the data stored on, redirected through, or processed by its technology resources. The Jasper School District encourages the use of these technology resources; however they remain the property of the Jasper School District and are offered on a privilege basis only. Throughout this policy, the term “staff” identifies full- and part-time employees, contractors, consultants, temporaries, student assistants, volunteers, retired annuitants, vendors and other users including those affiliated with third parties who access Jasper School District technology resources due to their job responsibilities. Management expects staff to comply with this and other applicable Jasper School District policies, procedures, and local, state, federal, and international laws. ***Failure to abide by these conditions may result in forfeiture of the privilege to use technology resources, disciplinary action, and/or legal action.***
The IT Policy Review Team regularly modifies this and other IT security related policies to reflect changes in industry standards, legislation, technology and/or products, services, and processes at the <company>.

Privacy
The Jasper School District reserves the right to monitor, duplicate, record and/or log all staff use of Jasper School District technology resources with or without notice. This includes but is not limited to e-mail, Internet access, keystrokes, file access, logins, and/or changes to access levels. ***Staff shall have no expectation of privacy in the use of these technology resources.***

Liability
The Jasper School District makes no warranties of any kind, whether expressed or implied for the services in this policy. In addition, the Jasper School District is not responsible for any damages which staff may suffer or cause arising from or related to their use of any Jasper School District technology resources. ***Staff must recognize that Jasper School District technology resource usage is a privilege and that the policies implementing said usage are requirements that mandate adherence.***

Staff Responsibilities and Accountability
Effective information security requires staff involvement as it relates to their jobs. Staff is accountable for their

actions and therefore they own any event(s) occurring under their user identification code(s). It is staff's responsibility to abide by policies and procedures of all networks and systems with which they communicate. Access of personal or private Internet Service Providers while using Jasper School District provided information technology resources or using non-Jasper School District provided information technology resources to conduct Jasper School District business does not indemnify any entity from the responsibilities, accountability and/or compliance with this or other Jasper School District policies. Staff responsibilities include but are not limited to:

- Access and release only the data for which you have authorized privileges and a need to know (including misdirected e-mail)
- Abide by and be aware of all policies and laws (local, state, federal, and international) applicable to computer system use
- Report information security violations to the Information Security Officer or designee and cooperate fully with all investigations regarding the abuse or misuse of state owned information technology resources
- Protect assigned user IDs, passwords, and other access keys from disclosure
- Secure and maintain confidential printed information, magnetic media or electronic storage mechanisms in approved storage containers when not in use and dispose of these items in accordance with Jasper School District policy
- Log off of systems (or initiate a password protected screensaver) before leaving a workstation unattended
- Use only Jasper School District acquired and licensed software
- Attend periodic information security training provided by Jasper School District IT Security Branch
- Follow all applicable procedures and policies

Electronic Mail (E-Mail) Policy

The Jasper School District electronic mail services (e-mail) policy provides staff with guidelines for permitted use of the Jasper School Districted-mail technology resource. The policy covers e-mail coming from or going to all Jasper School District owned personal computers, servers, laptops, paging systems, cellular phones, and any other resource capable of sending or receiving e-mail.

Ownership

The Jasper School District owns all e-mail systems, messages generated on or processed by e-mail systems (including backup copies), and the information they contain. Although staff members receive an individual password to access the e-mail systems, e-mail and e-mail resources remain the property of the Jasper School District.

Monitoring

The Jasper School District monitors, with or without notice, the content of e-mail for problem resolution, providing security, or investigative activities. Consistent with generally accepted business practices the Jasper School District collects statistical data about its technology resources. Jasper School District technical staff monitors the use of e-mail to ensure the ongoing availability and reliability of the systems.

Accountability

Staff may be subject to loss of e-mail privileges and/or disciplinary action if found using e-mail contrary to this policy. Staff must maintain the confidentiality of passwords and, regardless of the circumstances, ***never share or reveal them to anyone***. The Information Security Officer (ISO) must provide express written permission before sensitive information is forwarded to any party outside of the Jasper School District. Staff should contact the ISO with questions regarding the appropriateness of information sent through e-mail.

Ethical Behavior and Responsible Use

The Jasper School District provides e-mail systems to staff to facilitate business communications and assist in performing daily work activities.

Ethical and Acceptable

- Communications and information exchanges directly relating to the mission, charter, and work tasks of the Jasper School District
- Announcements of laws, procedures, hearings, policies, services, or activities

- Notifying staff of Jasper School District sanctioned employee events, such as the holiday party, bake sales, arts and craft fairs, retirement luncheons, and similar approved activities
- Respecting the legal protection provided by all applicable copyrights and licenses
- Practicing good housekeeping by deleting obsolete messages

Unethical and Unacceptable

- Violating ***any*** laws or Jasper School District policies or regulations (e.g. those prohibiting sexual harassment, incompatible activities, or discrimination)
- Submit, publish, display, or transmit any information or data that contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory, or illegal material
- Compromising the privacy of staff, customers, or data and/or using personal information maintained by the Jasper School District for private interest or advantage
- Engaging in any activities for personal gain, performing personal business transactions, or other personal matters (e.g. sending sports pool or other gambling messages, jokes, poems, limericks, or chain letters)
- Intentionally propagating, developing, or executing malicious software in any form (e.g. viruses, worms, trojans, etc.)
- Viewing, intercepting, disclosing, or assisting in viewing, intercepting, or disclosing e-mail not addressed to you
- Distributing unsolicited advertising
- Accessing non-Jasper School District e-mail systems (e.g. Hotmail, Yahoo!) using Jasper School District owned resources

Reinforces Family Educational Rights and Privacy Act (FERPA)

Family Policy Compliance Office (FPCO) Home

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However,

FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

School officials with legitimate educational interest;
Other schools to which a student is transferring;
Specified officials for audit or evaluation purposes;
Appropriate parties in connection with financial aid to a student;
Organizations conducting certain studies for or on behalf of the school;
Accrediting organizations;
To comply with a judicial order or lawfully issued subpoena;
Appropriate officials in cases of health and safety emergencies; and
State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For additional information or technical assistance, you may call (202) 260-3887 (voice). Individuals who use TDD may call the Federal Information Relay Service at 1-800-877-8339.

Or you may contact us at the following address:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-5920

1B. Standards

JASPER SCHOOL DISTRICT 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 or parents 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.

1B.A Risk Management

© 2002-2006 Carnegie Mellon University 1

Overview of Risk Management

© 2002-2006 Carnegie Mellon University 3

Overview

The purpose of this module is to familiarize employees with risk management. To do this, employees first must understand the key attributes of risk and the concepts underlying risk management (including risk analysis assessment). One of these key attributes is the valuation and determination of assets. In most organizations, this process consists of identifying and prioritizing assets based on their value, cost, or importance. This module focuses on organizations that select and prioritize assets based on the assets’ importance or relevance to fulfilling the mission and objectives of the organization.

This module also introduces concepts such as risk, risk impact, risk attributes, assets, asset categories, risk analysis, and risk management. Additionally, this section examines the application of risk management. This examination includes a description of risk assessment and analysis activities, comprehension of the impact of risk events, and recognition of mitigation strategies for managing and reducing risk.

Risk

Risk is the potential that a given threat will exploit vulnerabilities of an asset and compromise its CIA.

1.B.A.1 Description of Risk

Risk is the possibility of suffering harm or loss. With respect to information and computer data, risk is the potential that a given threat will exploit vulnerabilities to compromise an asset’s confidentiality, integrity, or availability.

Before risks can be managed, they must be identified. One way to identify potential risk is to list the components of risk in an asset-driven scenario and gauge the risk’s plausibility.

Example of Risk

For example, let's consider a home user making a consumer purchase over the Internet. In this situation, the user must submit customer information to the Web site (i.e., item, quantity, name of customer, address of customer, payment type, credit card number, etc.) to complete the purchase. Therefore, from the user's point of view (even if he or she is not explicitly aware of the risk or is seemingly unconcerned about it), risk exists. To identify the risk in this situation, we can state that the asset is the customer's information, the threat is anyone on the Internet with malicious intent, and the vulnerability is any technology weakness that allows the information to be observed and captured.

Threats and Vulnerabilities

Probably the most readily identifiable components of risk, to system and network administrators, are threat and vulnerability. The combination of threat and vulnerability yields a potential for undesirable outcomes, as when threats exploit vulnerabilities in an asset to compromise the asset's confidentiality, integrity, and/or availability. These undesirable outcomes are referred to as impacts.

Risk Impact

Compromising CIA of critical assets can cascade into loss of

- Key technologies
- Competitive position
- Customer confidence
- Trust
- Revenue
- Life or property
- Financial stability. monetary fine, law suit, or regulatory penalty

1.B.A.2 Risk Impact

Understanding a risk's impact forms the basis for evaluating outcomes of risk: loss, destruction, modification, and interruption. Impact is the actualization of risk. To evaluate the outcome of a risk, we start by developing evaluation criteria for risk scenarios.

For example, consider a home user who sets up a personal Web server to display his or her resume. As a risk management process, our home user identifies his or her assets, considers possible negative outcomes, and characterizes the potential impact of an asset's compromise. Here, our home user recognizes that one asset is the Web server itself, while another is his or her resume. Possible negative outcomes to the resume asset include

- Destruction of the resume file
- Modification of the resume content
- Pirating of the resume data
- Interruption of the resume's presentation to the Internet

After considering these potential negative impacts, our home user should be able to define potential failure conditions, such as

- Destruction, causing an expenditure of effort to restore or recover the information
- Modification, causing a prospective employer to consider the candidate either adequate or inadequate for the position, depending on what information was changed

- Theft, causing a loss of creative and competitive marketing of the individual's skills or background
- Interruption, causing an inability for potential employers to view the candidate's information

Finally, the home user must decide whether he or she really cares about the potential impacts to his or her assets. If yes, then mitigation strategies should be supplied; if no, then the potential risk impacts are accepted in addition to the consequences of loss or harm that could be suffered through exposure to the risk.

Components of Risk

RISK Asset
Threat Vulnerability

1.B.B Components of Risk

For a risk to exist, the following must be present:
- Assets of value to an organization or individual that must be protected (critical assets)
- Threats to these critical assets (possibility of disclosure, modification, destruction, or interruption)
- Vulnerabilities of these critical assets that may provide an opportunity for threats to act on the assets in a manner that discloses, modifies, destroys, or interrupts the assets

Identifying assets involves a discussion within the organization to determine what categories of assets exist, who owns each asset, and what level of protection is necessary for each asset. This exchange of information should take place between managers, staff, and information technology personnel on a periodic basis and as part of the organization's review of its information security policy. These events are important as a means of identifying assets and risk mitigation plans because they enable the organization to identify its current protection strategy for each asset and any changes to the asset's priority. This priority discussion allows a ranking of some assets over others, and it should be documented and reflected in organizational policy, recognizing that assets may be mission critical, non-critical but sensitive, or general in nature.

Relating threats and vulnerabilities to an asset is part of risk assessment and requires that those responsible for protecting information assets have an appreciation of the range of threats and vulnerabilities. Once the range is known, the likelihood of any one threat acting adversely on an asset must be understood.

The results of risk analysis identify the strategies (plans, policies, technological mechanisms) that can help mitigate the risk. Analysis includes evaluating the risk to an organization and measuring that risk against the impact to the organization if the risk is realized. For example, a determined risk for a medical organization may be that "modification of paper medical records by unauthorized individuals can lead to loss of life, financial or punitive penalties, or loss of customer confidence." In this case, this risk is actually stated as a risk scenario that includes assets (paper medical records), threat actors (personnel exceeding their privileges or unauthorized outsiders), outcome (modification of the records), and impact (public safety, financial, customer confidence, legal). Risk analysis determines which risks are viable (that is, non-negligible) and what degree of impact (high, medium, or low) the risk has on the organization when evaluated.

1.B.C Identify Assets

An asset is anything of value to an organization. Typically, assets are classified as information assets (people, hardware, software, systems), other supporting assets (facilities, utilities, services), or critical assets. Critical assets may include information or other supporting assets. Later in this section, we will describe examples within each category.
It is important to note that your organization may choose to classify assets within different categories according to sensitivity or function. Asset definitions may be highly subjective, and asset value even more so; therefore, an easier way to approach assets and asset value can be to consider the worth of the asset (in both tangible and intangible terms) to the organization. By examining the costs associated with the value and intrinsic value of an asset (qualities of the asset's existence), you may discover a more meaningful definition and value of the asset.

Information includes

- data being processed on, stored on, or transmitted between systems
- backup and archive data (on-site and off-site storage volumes and locations)
- paper documents
- escrowed encryption keys
- software distribution media

Hardware includes

- desktop computers
- servers
- mainframes
- network equipment (routers, switches, firewalls)
- wiring infrastructure
- wireless support infrastructure

Software includes

- commercial off-the-shelf (cots) software

− operating systems
− desktop software
− mainframe applications

- custom software

− in-house effort
− outsourced effort
− ad hoc scripts
− undocumented tools used by employees

People include

- senior and middle management
- technical and non-technical staff
- public relations
- help desk, facilities, security

• contractors, third parties (Computer Security Incidence Response Teams [CSIRTs])
• government, police, fire

Facilities include
• heating/ventilation/air conditioning (hvac) support
• power
• water
• telephone
• security

Utilities include
• power
• water
• telephone
− leased lines (t1, t3, isdn)
− voice lines
− cell phones
• pager services
• service-level agreements
− hardware maintenance
− HVAC support

Outsourced services include
• off-site services
− information storage
− Web services
• consultants
• utilities
• legal services
• public relations
• managed or monitored security
− physical
− network

Identify Critical Assets

Critical Assets are assets determined to have an integral relationship with the mission of the organization and its success.

Examples:

- Intellectual property /patents / copyrights
- Corporate financial data
- Customer sales information
- Human resource information

1.B.C.1 Identify Critical Assets

Critical assets are assets that have an integral relationship with the mission of the organization. This means that loss or damage to a critical asset would cause disruption to the operational or functional mission of the organization to a point where the mission fails. This concept recognizes that each individual organization will define a different and unique set of critical assets that align with mission success or failure.

Examples of critical assets include

• intellectual property
− patents, copyrights
− software code under development
− systems acquisition or
development projects
• corporate financial data
− payroll information by employee, department, organization
− financial earnings, revenue, and loss statements
− stock dividend information
• customer sales information
− names, addresses, credit card /account numbers, purchase histories, demographic information
• human resource information
− names of employees, departments, salaries
− hiring, administrative punishment, and disability information
• network architecture information
− network topology diagrams
− desktop or systems replacement plans
− strategic infrastructure plans
− vulnerability assessment reports
− types and locations of infrastructure (general purpose, storage, server, networking, and security devices)
• U.S. Government or state government classified information
− compartmentalized projects
− deployment and strategic plans
− intelligence information, logistic movements/support
− technical specifications on equipment, weapons, projects

Identify Security Requirements

Each critical asset has different requirements of confidentiality, integrity, and availability that should be

- Documented
- Communicated

1.B.C.2 Identify Security Requirements

Each critical asset has different requirements for *confidentiality*, *integrity,* and *availability* that should be

• documented, describing the requirements, the responsible information/asset owner(s), and the party charged with the asset’s protection, as well as under what conditions and to what degree the requirements must be enforced

• communicated throughout the organization, especially from the owner of the asset to the person(s) responsible for its safety and security (the information/asset custodian)
Security requirements should be understood at all levels of the organization involved in the asset's protection. They should be described with enough detail for a specific requirement to be placed on the responsible owner (manager, user, system/security administrator, etc.) or the technology protecting the asset. They should be documented in security policies and plans.

Vulnerabilities

Weaknesses in an asset

- Software Weaknesses
- Weak default settings

Default accounts/passwords, access controls, unnecessary software

- Bugs
- Buffer overflows, poor error handling
- Architecture Weaknesses
- Single points of failure
- Personnel Weaknesses
- Lack of awareness/training

1.B.C.3 Vulnerabilities

Vulnerability is the absence or weakness of a safeguard. It can also be described as a weakness in an asset or in the methods of ensuring that the asset is survivable. The examples of vulnerabilities listed on this slide provide a small sampling of the numerous classes of vulnerabilities that commonly exist.

Threats

Events that may compromise the CIA of an asset (i.e., exploitation of vulnerabilities)
Common threat tools/techniques:

- Malicious Code
- Worms, Viruses, Trojans, DoS
- Social Engineering
- Packet Sniffing and Network Scanning

1.B.C.4 Threats

A threat is any event that will cause an undesirable impact or loss to an organization if it occurs. Examples of threats include the following:
• intrusions into and disruptions of information systems
− viruses, worms, and Trojan horses
− denials of service
− sniffing network traffic
− stealing data assets
• loss of assets that are single points of failure
− critical data that is not backed up
− a single, critical piece of network infrastructure (i.e., a core router)
• keys that are used to encrypt critical data

Calculating Risk Exposure
Qualitative Risk Analysis

- Probability x Severity
- Risk Assessment Matrix

Quantitative Risk Analysis

- Potential Financial Loss

1.B.D Calculating Risk Exposure

Risk analysis is the process of identifying security risks, determining their magnitude, and identifying areas in need of safeguards. Risks are traditionally captured as a description that can then be measured both qualitatively and quantitatively. Qualifying a risk means understanding the potential negative impact with respect to the asset as well as the likelihood of the threat. This impact occurs when the asset is destroyed, modified, interrupted, or disclosed. To home users, qualifying risk often means evaluating the impact of having their personal information disclosed. In this case, the users will probably be most concerned with their financial liability, chance of identity loss, and laws and regulations to which they may be subjected, as established by a qualitative scale (or criteria) for evaluating the risk (such as high, medium, or low).

Quantifying risk means understanding the possibility of the risk existing or coming to fruition. Here the home user attempts to measure the probability or likelihood of someone performing several different attacks whose goals are to retrieve his or her personal information. This measurement takes into account how likely it is that

- someone may observe the information in transit between the home user and the Web site (and possibly decode the encrypted network traffic)
- the software making the exchange of personal information is vulnerable to attack
- the user will be singled out for exploitation over all of the other Web commerce transactions happening at the Web site of purchase
- an attacker might gain access to the information once it has arrived at the Web site

These are just a small sample of the risks involved in this simple transaction. For the individual to really understand these risks, he or she must appreciate the potential impact of these risks. This demands an understanding of the potential that threat sources (humans, system problems, viruses, etc.) have in exploiting and abusing vulnerabilities that result in risk. This potential falls into a continuum ranging from negligible to actual, over the life of the information being transmitted, stored, and processed.

Quantitative risk analysis can be a major project and can consume considerable organizational resources. It attempts to assign independently objective numeric values (hard dollars, for example) to the components of risk assessment and to the assessment of potential losses. Qualitative risk analysis addresses more intangible values of loss and typically attempts to produce scenarios so risk can be anticipated and managed. However, threat frequency and impact data is still required to conduct a qualitative risk analysis.

Use exposure values to:

. **Prioritize the order in which risks are addressed**
. **Help in deciding how to manage risks**
A new worm attacks vulnerable systems

Web site defacement
Datacenter flooded by fire protection system

Qualitative Risk Analysis

1.B.D.1 Qualitative Risk Analysis

Exposure Factor (EF)

- % of loss of an asset

Single Loss Expectancy (SLE)

- EF x Value of asset in $

Annualized Rate of Occurrence (ARO)

- A number representing frequency of occurrence of a threat. Example: 0.0 = Never 1000 = Occurs very often

Annualized Loss Expectancy (ALE)

- Dollar value derived from: SLE x ARO

3.4.2 Quantitative Risk Analysis

Managers in IT are often faced with the dilemma of justifying their expenditures on survivability and security. Ideally, resources allocated toward survivability should be seen as an investment in the mission of the organization. But because the old paradigm (security seen as an overhead expense) is still an operational reality, IT managers often justify expenditures with forms of quantitative risk analysis. The terms shown on this slide are pseudo-standards that can help calculate risk in relation to actual dollar figures. Their usage helps to provide more reliable cost-benefit analysis.

• Exposure Factor (EF)

The exposure factor describes the effects a realized threat would have on a particular asset as a percentage of loss of the total value of the asset. For example, loss of some hardware would have a small EF, whereas the catastrophic loss of all computing resources would have a large EF. The EF value is necessary to compute the Single Loss Expectancy (SLE), which in turn is necessary to compute the Annualized Loss Expectancy (ALE).

• Single Loss Expectancy (SLE)

The single loss expectancy is the dollar figure assigned to an organization’s loss from a single threat event. It is derived from the formula EF X asset value in dollars = SLE. For example, an asset valued at $10,000 that is subjected to an EF of 50 percent would yield an SLE of $5,000.

• Annualized Rate of Occurrence (ARO)

The annualized rate of occurrence is a number that represents the estimated frequency with which a threat is expected to occur. This value can range from 0.0 (for threats that never occur) to a large number (for threats that occur frequently, such as misspellings of names in data entry). This number is usually created based on the likelihood that the threat will occur and the number of individuals that could cause it to occur. The loss incurred by this event is not a concern here, only how often it occurs.

• Annualized Loss Expectancy (ALE)

Annualized loss expectancy (ALE) is the annual financial loss an organization expects from a threat. It is calculated by multiplying the single loss expectancy and annualized rate of occurrence (SLE X ARO = ALE). For example, a threat with a dollar value of

$10,000 (SLE) that is expected to occur 5 times per year (ARO) will result in an ALE of $50,000 [Krutz 2001].
Generally speaking, if an organization's information survivability expenditures are less than the sum of the calculated ALEs, than some quantitative return on investment (ROI) figures can be discerned.

Summary of the Assessment Step
Risk is the probability and severity of loss from exposure to a threat. The assessment step involves the application of quantitative or qualitative measures to determine the level of risk associated with a specific threat. Specifically, this process evaluates the probability and severity of an undesirable event that could result from the threat.

Risk Management

Process of assessing and quantifying risk and establishing an acceptable level of risk for the organization

Risk can be mitigated, but cannot be eliminated.

1.B.E Risk Management
Risk management should be a well-defined and established process. Effective risk management can save resources, reduce mishaps, and even save lives.

Managing Risks
Acknowledge that the risk exists, but apply no safeguard (Exposure value is within tolerance)
Shift responsibility for the risk to a third party (ISP, MSSP, Insurance, etc.)
Change the asset.s risk exposure (apply safeguard) Eliminate the assets exposure to risk, or eliminate the asset altogether.

1.B.E.1 Risk Management Strategies
Organizations have four options when deciding how to manage risks:
1. Accept
If an organization chooses to accept risk, it does so with full knowledge of the potential threats and vulnerabilities to the asset. It may be that the asset's exposure is acceptable or within some level tolerance. For example, an organization recognizes the threat that usernames and passwords could be compromised by administering systems remotely with telnet, a protocol that transmits data, including passwords, in plaintext. However, the organization decides the risk is not great enough to warrant a safeguard (i.e., encrypted sessions with SSH or IPSec).
2. Mitigate
Mitigating risk is the process of actively applying safeguards to reduce an asset's level of exposure. In the above telnet example, the organization could mitigate the risk by (a) denying all management traffic to the remote systems that is not encrypted and authenticated, and (b) writing an organizational policy that acts as a deterrent (i.e., any attempt to compromise access controls on organizational systems will be met with stiff disciplinary action).

3. Transfer

Transfer of risk occurs when an organization decides to contract with a third party to mitigate the risk. For example, an organization can transfer the risk of losing data (and support the goal of mission survivability) by contracting with a service provider that maintains an off-site data backup and recovery capability. Although risk transference does not change the probability or severity of a threat, it may decrease the probability or severity of the organization's risk. At a minimum, the organization's risk is greatly decreased or eliminated because the possible losses or costs are shifted to another entity.

4. Avoid

Avoiding risk means that the organization eliminates the asset's exposure or even the asset itself. An example might be the replacement of historically vulnerable platforms (like Internet Information Server) with hardened platforms like a Bastille/Apache Web server solution [Bastille 06].3F

4 See http://www.bastille-linux.org/.

Summary

Risk

- The possibility of compromising an asset.s CIA
- Composed of assets, threats, and vulnerabilities
- Exposure measurement may be qualitative or quantitative
- May be avoided, accepted, mitigated, or transferred
- Can be mitigated, but never eliminated

1.B.F Summary

Sustaining and improving information security is a continuous risk management activity.

Risk is comprised of assets (something of value to the organization), threats (concerns related to undesirable outcomes), safeguards, and vulnerabilities (weaknesses creating the possibility for threats to negatively impact the organization).

Risk analysis, a major component of risk assessment, helps to identify the possibility of certain risks and the impact when risks are realized. Because information cannot be realistically managed to have no risk, at some point risk must be accepted.

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

1B3 TRAINING

JASPER SCHOOL DISTRICT, 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. As stated in the Jasper School District Technology Plan, staff development and training will be as follows:

Staff Development and Training

The technology plan must include strategies for providing ongoing professional development for teachers and administrators in the integration of technology with curriculum and school management.

Staff development to teachers and administrators in the use of technology for delivery of education will be provided through training on the use of a variety of software which will be used to maximize delivery of instruction through PowerPoint, Word, Excel, and other programs. Staff will also be trained in the use of software to analyze and disaggregate information regarding student achievement. They will also be made aware of avenues of research which are available through internet use.

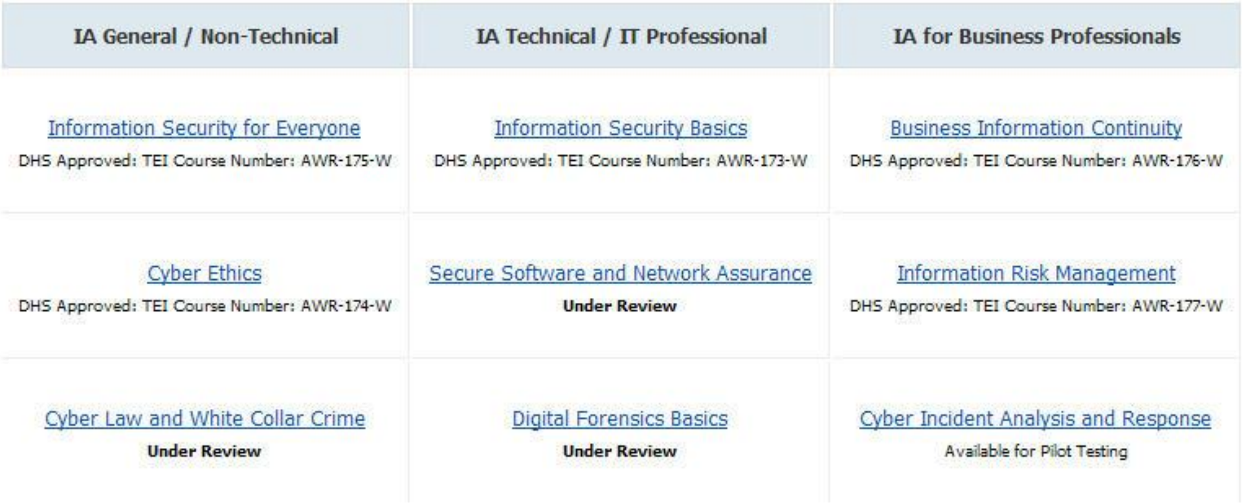
Technology is being used to facilitate instruction through distance learning, server based applications, and various other web-based instructions.

The Jasper School District has adopted technology skills standards at the local level for teachers, administrators, or public library staff. These standards developed based on any nationally-based standards such as the International Society for Technology in Education (ISTE) or other models.
School staff is sufficiently trained to integrate technology with instruction and is assessed on the effectiveness of training through survey and observation of the use of technology in the classroom.

School administrators are sufficiently trained in the use of technology as an administrative tool. Administrators are assessed on their training through survey and observation of the use of technology in their administrative activities.

Training Resources:

1. ACT Online. Sponsored by Homeland Security. Provides several Free online Security Courses. https://www.act-online.net/
2.



IA General / Non-Technical	IA Technical / IT Professional	IA for Business Professionals
Information Security for Everyone DHS Approved: TEI Course Number: AWR-175-W	Information Security Basics DHS Approved: TEI Course Number: AWR-173-W	Business Information Continuity DHS Approved: TEI Course Number: AWR-176-W
Cyber Ethics DHS Approved: TEI Course Number: AWR-174-W	Secure Software and Network Assurance **Under Review**	Information Risk Management DHS Approved: TEI Course Number: AWR-177-W
Cyber Law and White Collar Crime **Under Review**	Digital Forensics Basics **Under Review**	Cyber Incident Analysis and Response Available for Pilot Testing

3.

1. Kym Patterson, Arkansas State Chief Security Officer, issues monthly newsletters, regarding Cyber Security. You can request to be added to the distribution list for the newsletter, which can then be dispersed to your staff. (email: kym.patterson@arkansas.gov) Many state agencies are using this to fulfill the training requirement.
2. The state security office has applied for a grant, that would provide funding to establish a more elaborate online training program.
3. http://staysafeonline.org/ provides Cyber Security Awareness lesson plans for K-12.
4. http://www.ed.gov/policy/gen/guid/fpco/brochures/elsec.html The United States Dept. of Education's website regarding K-12 FERPA.

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

JASPER SCHOOL DISTRICT 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. The District will implement, but is not limited to:

- Automatic screensaver after 15 minutes for teachers and students; APSCN users 5 minutes or less
- Automatic log off for students after 25 minutes
- Automatic shut off of each computer at the end of each day

JASPER SCHOOL DISTRICT 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.

- Secure device with TrueCrypt (encryption software)
- Redirect document folders to secured driver and lock C:/ drive from end users
- Lock all cellphones with security PIN

State of Arkansas Agency #200.00
Office of Information Technology
124 West Capitol Avenue Suite 990 Little Rock, AR 72201
Phone 501-682-4300 Fax 501-682-2040
http://www.cio.arkansas.gov/techarch

Standard Statement – Encryption

Title: Encryption
Document Number: SS-70-006
Effective Date: Upon the earlier of: 1) July 1, 2008; or 2) The line-item appropriation to the agency in question of funds to comply with the rule
Published by: Office of Information Technology

1.0 Purpose

Sensitive information held by public organizations can include social security numbers, credit card numbers, and other personal information about Arkansas' citizens. Government, in particular, is responsible for information that protects public health and public safety. Individuals with malicious intent can easily acquire information being transmitted electronically unless appropriate security measures are applied, such as encryption.

If detected, the credentials employees use to access data and systems can provide unauthorized access which can lead to critical data being modified, deleted and ultimately made unavailable. For these reasons very sensitive information must be protected through encryption methods.

2.0 Scope

This standard statement applies to all state agencies, administrative portions of institutions of higher education, boards and commissions.

3.0 Background

The Arkansas Information Systems Act of 1997 (Act 914, 1997) gives the Office of Information Technology the authority to define standards, policies and procedures to manage the information resources within the state. This is accomplished through work with a multi-agency working group known as the Shared Technical Architecture Team.

In addition, Act 1042 of 2001 states that the Executive Chief Information Officer oversees the development of information technology security policy for state agencies, boards and commissions and administrative portions of institutions of higher education.

4.0 References

4.1 Act 914 of 1997: Authorized the Office of Information Technology (OIT) to develop statewide policies.

4.2 Act 1042 of 2001: Authorized the Executive CIO to develop security policy.

5.0 Standard

5.1 The following standard applies only to data that is classified by the SS-70-001 Data and System Security Classification Standard as being Level C - Very Sensitive or Level D - Extremely Sensitive and transmitted on a public network, including the state network, or removed from a covered entity's physical location

5.1.1 Users accessing data from outside organizational local area networks must encrypt their credentials, including login IDs and passwords, to access such data.

5.1.2 Data on all portable media and electronic devices, such as laptops, PDAs, flash drives, CDs, DVDs, or any external storage device shall be encrypted. Compliance by covered entities with Section 5.1.2 shall be achieved upon the earlier of: 1) July 1, 2008; or 2) The line-item appropriation to the agency in question of funds to comply with the rule.

5.1.3 Backups for business continuity purposes that are taken offsite shall be encrypted. Compliance by covered entities with Section 5.1.3 shall be achieved upon the earlier of: 1) January 1, 2009; or 2) The line-item appropriation to the agency in question of funds to comply with the rule.

5.1.3.1 Archived backups created prior to the effective date of this standard are exempt from this encryption requirement and are subject to the requirements of the Physical and Logical Security Standard (SS-70-008).

5.1.3.2 Encryption keys used to encrypt data used for business continuity purposes must be stored offsite within a locked or otherwise restricted environment in a building. Data shall be encrypted with algorithms utilizing 128 bit encryption, at a minimum.

5.1.4 Acceptable methods of 128 bit or higher encryption include, *but are not limited to*:

5.1.4.1 Triple-DES

5.1.4.2 Advanced Encryption Standard

5.1.4.3 International Data Encryption Algorithm (IDEA)

5.1.4.4 RSA (key length must be 1024 bits or higher)

5.1.4.5 SSL (secure socket layer)

5.1.5 Unacceptable encryption methods include, *but are not limited to*:

5.1.5.1 DES (Data Encryption Standard)

5.1.6 Encryption shall be used for data transmissions such as FTP (file transfer protocol) and Telnet. Methods of acceptable encryption include, but are not limited to, SSH, third party secure FTP solutions, and the use of a virtual private network.

6.0 Procedures

The State Security Office reserves the right to audit for compliance with this standard. Furthermore, the State Security Office has the right to grant an exception or exclusion to any part of this standard. With thirty days written notice, the State Security Office reserves the right to update the unacceptable encryption methods list as defined in Sections 5.1.5.

Covered entities may request an extension to come into compliance with any part of this standard by contacting the State Security Office with an expected compliance date. The State Security Office must approve all extension requests.

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

2B2 COMPUTER ROOM SECURITY

JASPER SCHOOL DISTRICT shall ensure that computer 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.

- Keeping servers and router locked in a secured room from end users.
  - *Applies to all servers that are part of a tree or domain.*
  - *Servers should not be in public areas.*
  - *A cage or locked rack would suffice in most situations.*
- Using manageable switches to block certain MAC addresses

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

JASPER SCHOOL DISTRICT 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.

- Network diagram showing cabling and end devices
- Static IP addresses and those ports that are open on the firewall.
- Sitebook including all devices such as: servers, workstations, routers, switches, printers, etc. *A simple (minimum requirements) template for site notebooks can be downloaded from: ftp://disftp.state.ar.us/pub/SiteNotebooks/*

JASPER SCHOOL DISTRICT 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.

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

3B2 WIRELESS NETWORKS

JASPER SCHOOL DISTRICT 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.

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

JASPER SCHOOL DISTRICT shall scan for (and disable) rogue wireless devices at a minimum quarterly.

Standard Statement – Wireless Security

Title: Wireless Security
Published by: Office of Information Technology

1. Purpose

Wireless technology gives users the ability to access data and applications from more locations in a cost effective manner, but wireless technology also presents problems in terms of security. All information assets handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. For these reasons, appropriate security measures are essential when deploying wireless technology *with access to the state network*.

2. Scope

This standard statement applies to all state agencies, administrative sections of institutions of higher education, boards and commissions.

3. Background

The Arkansas Information Systems Act of 1997 (Act 914, 1997) gives the Office of Information Technology the authority to define standards, policies and procedures to manage the information resources within the state. This is accomplished through work with a multi-agency working group known as the Shared Technical Architecture Team.
In addition, Act 1042 of 2001 states that the Executive Chief Information Officer oversees the development of information technology security policy for state agencies.

4. References

4.1 Arkansas State Government Information Resources Security Policy Guidelines

4.2 *Act 914 of 1997*: Authorized the Office of Information Technology (OIT) to develop statewide policies

4.3 *Act 1042 of 2001*: Authorized the Executive CIO to develop security policy.

4.4 Encryption Standard: http://www.cio.arkansas.gov/techarch/indexes/standards.htm

5. Standard

5.1. All configuration parameters (such as Service Set Identifier (SSID), keys, passwords, etc.) of Wi-Fi access points or bridges that can be changed from the default manufacturer settings shall be changed from the default. The beacon interval on the these Wi-Fi access points should be set to the longest interval possible. Where applicable, the new settings should be complex.

5.2. Wireless hotspot networks may exist on the state network if and only if the following are met:

5.2.1. The Service Set Identifier is changed to one which appropriately identifies the wireless network as a hotspot environment.

5.2.2. A secure method exists to identify and authenticate users of the hotspot environment such as a captive web portal. Appropriate audit logs containing IP address, login id, and logon/logoff date and time stamps should be maintained based on the organization's data retention policy.

5.2.3. Systems or applications which contain data which is classified by the SS-70-001 Data and System Security Classification Standard as being Level B - Sensitive, Level C - Very Sensitive or Level D - Extremely Sensitive must have appropriate access controls (firewall rules, router access control lists, and similar measures) that disallow wireless hotspot users from directly accessing the system or application.

5.2.4. Users of the hotspot environment which require access to systems or applications classified Very Sensitive or Extremely Sensitive must use appropriate technology such as VPN, secure shell, SSL/TLS encrypted webpages and similar authenticated and encrypted technology to access these resources in accordance to SS-70-009 Remote Access standard and the SS-70-006 Encryption standard.

5.2.5. Appropriate warning banner is presented to authorized and unauthorized users of the hotspot environment captive portal in accordance to SS-70-003 Warning Banner. Hotspot users must be given opportunity to view any appropriate "acceptable use policy" and must agree to this policy as a part of authenticating via the captive portal.

5.2.6. Access to any Internet resources are denied to hotspot users until the authenticated to the wireless network through use of appropriate firewall or other access control mechanisms.

5.3. Covered entities which use wireless networking in a non-hotspot environment must adhere to the following.

5.3.1. Service Set Identifier must not contain information relative to agency location, mission, or name.

5.3.2. Wi-Fi equipment shall be configured for infrastructure mode only.

5.3.3. All wireless transmissions between a state network entity's wireless access point or bridge and clients shall be encrypted utilizing the WPA protocol at a minimum to prevent unauthorized access to the state network.

5.3.4. WEP (wireless encryption protocol) shall not be utilized due to its multiple security flaws.

5.3.5. Wirelessly transmitted data and credentials granting access to state resources are subject to SS-70-009 Remote Access and SS-70-006 Encryption standards.

5.4. Covered entities will search for and disable rogue Wi-Fi access points to the state network quarterly, at a minimum.

5.5. Covered entities utilizing wireless technologies shall establish a policy to ensure compliance with the state wireless security standard.

5.6. Wireless networks that covered entities may use that are separate from the state network are not subject to this standard. Clients, however, must still adhere to SS-70-009 Remote Access and SS-70-006 Encryption standards when accessing Level B, C or D data from these outside environments.

5.7. Bluetooth wireless devices must be secured to the extent configurable between the devices involved.

6. Procedures

The State Security Office reserves the right to audit for compliance with this standard. Furthermore, the State Security Office has the right to grant an exception or exclusion to any part of this standard. The Arkansas Division of Legislative Audit also audits for compliance with this standard.

7. Revision History

8. Definitions

8.1 Bluetooth Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers, and personal digital assistants (PDAs) can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection.

8.2 Hotspot A public or semi-public wireless local area network (WLAN) that provides Internet access to subscribers

8.3 Rogue Access Point Unauthorized wireless device allowing access to the state network

8.4 SSID (Service Set Identifier) A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN). This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.

8.5 State Network The state core information technology infrastructure serving Arkansas agencies, boards, commission, public schools, institutions of higher education, libraries, and other public organizations with Internet connectivity, data processing and transmission, video conferencing and telecommunications

8.6 WEP (Wired Equivalent Privacy) WEP (Wired Equivalent Privacy) - WEP is an optional privacy protocol originally specified in the IEEE 802.11 (802.11 legacy) standard that is designed to provide a level of security and privacy comparable to what is usually expected of a wired LAN. Weakness in the design make this protocol unsuitable for use in environments which must protect sensitive data.

8.7 Wi-Fi A term used to describe the underlying technology of wireless local areal networks (WLAN) based on the IEEE 802.11 set of specifications and is used interchangeably with the term wireless. Wi-Fi refers to any individual standard or the collection of all standards within the 802.11 family such as 802.11a, 802.11b/g, 802.11i or 802.11n.

8.8 Wireless Wireless LAN (local area network) data access technology including the following protocols: 802.11 series and Bluetooth that accesses state information technology resources.

8.9 WLAN (wireless local area network) A communication system that enables mobile users to connect to a wired network through a wireless (radio) connection, often implemented as an extension to wired LAN. WLAN's are typically found within a small client node, dense locale (e.g. a campus or office building), or anywhere a traditional network cannot be deployed for logistical reasons.

8.10 WPA (Wi-Fi Protected Access) WPA is a security standard for users of computers equipped with Wi-Fi wireless connection. It is an improvement on and is expected to replace the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). WPA provides more sophisticated data encryption than WEP and also provides user authentication.

9. Related Resources

9.1. FCC Wireless Website: http://wireless.fcc.gov/

9.2. SANS website: www.sans.org

9.3. Bluetooth website: www.bluetooth.com

9.4. Wi-Fi Alliance website: www.wifialliance.org

10. Inquiries Direct inquiries about this standard to:
Office of Information Technology
Shared Technical Architecture
124 W. Capitol Ave., Suite 990
Little Rock, AR 72201
Voice: 501-682-4300
FAX: 501-682-2040
Email: sharedarchitecture@arkansas.gov
OIT standards can be found on the Internet at:
http://www.techarch.state.ar.us

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

3B3 REMOTE ACCESS

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

- ***This especially applies to APSCN users working from home or off site. Districts can purchase VPN accounts from DIS for APSCN users to be able to work from home. The cost is $5 per account.***
- ***Accounts cannot be shared.***

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

3B4 WARNING BANNERS

JASPER SCHOOL DISTRICT shall ensure that appropriate WARNING BANNERS have been implemented for all access points to the District internal network. The banners will appear first on all workstations (staff and student) apprising the user of the Jasper School District policy on use.

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

JASPER SCHOOL DISTRICT shall enforce strong password management for employees and contractors as specified in Arkansas State Security Office Password Management Standard.

- ✓ Unique user accounts/IDs which must never be shared (exception allowed for students below fourth grade).
- ✓ Secret eight character password length, known only to the user.
- ✓ Complex syntax such as alpha-numeric and special characters.
- ✓ Password expiration not-to-exceed ninety days.
- ✓ Prohibited re-use of most recent four passwords.
- ✓ Passwords encrypted on disk.
- ✓ Initial user passwords should be distributed as one-time (expired) passwords.

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

- ✓ Unique user accounts/IDs which must never be shared (exception allowed for students below fourth grade).
- ✓ Secret eight character password length, known only to the user.
- ✓ Complex syntax such as alpha-numeric and special characters.
- ✓ Password expiration not-to-exceed ninety days.
- ✓ Prohibited re-use of most recent four passwords.
- ✓ Passwords encrypted on disk.
- ✓ Initial user passwords should be distributed as one-time (expired) passwords.

4B2 SYSTEM ACCESS CONTROLS – authorization

JASPER SCHOOL 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.

JASPER SCHOOL 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

JASPER SCHOOL 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

JASPER SCHOOL DISTRICTS shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties. The District will implement, but is not limited to:

- Limit administrative access to only the districts ISO
- Will not allow any student to access a computer with APSCN
- Will enforce disciplinary actions upon users that share logon information.

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

JASPER SCHOOL DISTRICT 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

JASPER SCHOOL 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

JASPER SCHOOL DISTRICT shall develop and maintain an incident response plan to be used in the event of system compromise which shall include:

- ✓ Emergency contacts (i.e. vendors, DIS, ADE/APSCN, law enforcement, employees, etc.).
- ✓ Incident containment procedures.
- ✓ Incident response and escalation procedures.
- ✓ Business Continuity of Operations Plan
- ✓ Acceptable Use Agreement

- *NIMS (National Incident Management Systems) courses are provided free of charge from FEMA. The courses are web-based, the ICS 100 and ICS 700 are basic courses and familiarize staff with basic incident management structure.* *http://www.fema.gov/emergency/nims/NIMSTrainingCourses.shtm*
- *DIS COOP (Continuity of Operations Planning) group can provide training in using LDRPS ((Living Disaster Recovery Planning System) software to develop comprehensive disaster response plans. The software is web based and is no cost to schools to use.*

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

JASPER SCHOOL DISTRICT 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. *Identifying a second location does NOT mean you have to have a "hot site". A simple MOU (memorandum of understanding) with another school or COOP that you can use their facilities for restoration, in the event of a disaster.*
- ✓ 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

JASPER SCHOOL DISTRICT 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.

JASPER SCHOOL DISTRICT 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. JASPER SCHOOL DISTRICT will implement a special server/service called WSUS (Windows Server Update Services). A WSUS server, configured correctly, can force users to apply updates when they are released. A WSUS server also conserves precious bandwidth.

JASPER SCHOOL DISTRICT 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.

Jasper School District

Technology Disaster Recovery Plan

Backup Policy and Procedures

Definition: A backup is a duplicate of data that is stored on the file server(s), external hard drives, network attached storage device, and/or workstation(s). The purpose of the backup is to be able to retrieve any information that might have been lost or destroyed for whatever reason (infected by virus, hard drive crash, natural disaster, etc). *Note: Backups are not run for the purpose of data archival.

Information Technology Staff members are responsible for running weekly backups of critical data on all of the servers located within the Jasper School District. IT staff members will monitor the status of the backup jobs. Backups will be labeled appropriately on backup drives with the date/version of the backup easily identifiable. Copies of backup jobs will be transferred onto drives/disk and stored in a secure location at an off-site location.

Faculty/Staff are responsible for doing backups on their own workstations. Backups may be performed by using Windows backup utility program, manually copying files, or by using specific backup utilities provided by various software programs. Jasper School District encourages all users to save data to their “home directories (H: Drive),” or “My Documents folder, which is synchronized to the H: Drive,” as those directories are included in routine backup jobs.

Disaster Preparation Procedures and Precautions

Faculty/Staff Workstations:

All personnel are responsible for their own data. Users are recommended to back up any data that they have on their recommended to back up any data that they have on their workstation to disks, USB drives, and/or external hard drives.

District Servers:

IT staff members will be responsible for backing up data on servers that side on-site. Servers located off-site, such as Edline, Renaissance Place, and APSCNGUI, are backed up by their respective companies. When possible, redundant servers should be utilized and located in different campus locations.

Uninterrupted Power Supply Units (UPS) units should be installed for each major server in the district.

Disaster Recovery Procedures

Office Personnel:

Should a disaster incapacitate a single campus within our school district, office/administrative personnel would be relocated to a different campus on-site. If a disaster cripples the entire district, office/administrative personnel would be relocated to the local COOP or a nearby school district to continue work on applications such as APSCN.

Teachers:

Web-based applications which are housed off-site, such as Edline/GradeQuick, are accessible from any location with an Internet connection. Therefore, teachers could access web-based applications from home, the COOP, or another school district.

Sensitive Data:

No sensitive data is located on-site. Financial, personnel, and student data are housed on APSCN (Arkansas Public School Computer Network) servers located in Little Rock. This data could be accessed through the local COOP or a neighboring school district.

IT Department Staff:

In the event that a disaster should destroy network servers, replacement servers would be purchased and data restored from backup copies. Assistance from the Department of Information Systems would be requested in rebuilding network file servers and restoring data. Should network cabling connecting campuses be destroyed, local vendors would be contacted for assistance in repairing/replacing cabling.

Approved by District Technology Committee—July 2009

Approved by Jasper School Board—July 2009

Jasper School District

Incident Response Plan

Section 1 – Incident Definition

An incident is any one or more of the following:
Loss of information confidentiality (data theft)
Compromise of information integrity (damage to data or unauthorized modification).
Damage to physical IT assets including computers, storage devices, printers, etc.
Denial of service.
Misuse of services, information, assets.
Infection of systems by unauthorized access.
Unauthorized changes to organizational hardware, software, or configuration.
Report of unusual system behavior.
Responses to intrusion detection alarms.

Section 2 – Incident Response

Any faculty or staff member who discovers a potential incident should contact the Jasper Technology Department by calling any of the following number:
(870) 446-2223 ext. 285

Once contacted, members of the technology department will meet and discuss the situation and determine a response strategy.
Is the incident real or perceived?
Is the incident still in progress?
What data or property is threatened and how critical is it?
What is the impact on the business should the attack succeed? Minimal, serious, or critical?
What system or systems are targeted, where are they located physically and on the network?
Is the incident inside the trusted network?
Is the response urgent?
Can the incident be quickly contained?
Will the response alert the attacker and do we care?
What type of incident is this? Ex.: virus, worm, intrusion, abuse, damage.
If not already done in step one, a work order will be created in the original reporter's name to document the incident report and to serve as a location for further communication and information about the incident. Technology department members will then develop a course of action to deal with the incident and ensure business continuity.
If needed, the Arkansas Department of Information Systems will be contacted at 1-800-435-7989 to help with this process.

Technology department members will restore the affected system(s) to the unaffected state.
They may do any or more of the following:
Purchase replacement workstations or servers if systems are damaged beyond repair.
Repair or replace any damaged networking hardware or wiring.
Re-install the affected system(s) from scratch or restore data from backups if necessary.
Preserve evidence before doing this.
Make users change passwords if passwords have been sniffed.
Be sure the system has been hardened by turning off or uninstalling unused services.
Be sure system is fully patched.
Be sure real time virus protection and intrusion detection is running.

If during this course of action, it is deemed that the incident might be of a criminal nature the Jasper School District will contact local/state authorities for support and consultation.

<u>Section 3 – Incident Review</u>
Forensic techniques including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, interviewing witnesses and the incident victim will be used to determine how the incident was caused.
Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

Assess the damage to the organization and estimated both the damage cost the cost of the containment efforts.

Review response and update policies – Plan and take preventative steps so the intrusion can't happen again.

Technology Phone Tree

Kerry Saylors
Superintendent
(Cell) 870.204.0078

Margie Rutledge
Technology Coordinator
(Cell) 501.622.0806

Stacy Liles
APSCN Support
501-944-8573

Warren Gatrel
Lead Tech
501-231-3137

OUR COOP
Nathan Cline
Technology Admin
870-

DIS Call Center
1-800-435-7989
Dis.callcenter@arkansas.gov

Claire Bailey
DIS Director
501-682-5148

Rick Martin
DIS Network Engineer
501-682-2403

Dana Thompson
APSCN Field Technician
501-682-3637

Greg Allison
DIS Security
501-682-4008

Max Kolstad
Distance Learning
501-682-5097

Ed Byrnes
DIS Asset Manager
501-682-4839

Nanette Harrell
ADE Program Management
501-682-5201

Tri-County Telephone (Ritter)
800-758-5790

Madison County Telephone
479-738-2121
Repair Service: (479) 738-2121
After Hours: (479) 738-6611

Centurytel Telephone
Business: 866.768.1847
Repairs: 800.824.2877

MEMORANDUM OF UNDERSTANDING
BETWEEN

__________JASPER SCHOOL DISTRICT __________
AND
__________AGENCY B__________

The ___Jasper School District and _______Agency B___________ mutually consent to enter into this Agreement which forms the basis of this Memorandum.

1. PURPOSE

This Agreement between _____ Jasper School District and _______Agency B_________ establishes a framework of cooperation to ensure continuity of operations in the event that office space becomes uninhabitable. This document is not meant to be legally binding; it is a statement of cooperation between these two parties for future accommodations due to emergency/disaster declarations.

2. PRINCIPLES OF COOPERATION

a. ___Agency B________ agrees to allow Jasper School District_________ use of specific areas of _____(e.g. Gym at 123 Main)___________________________________ as an alternate location.

b. In the event that _Jasper School District___ must temporarily relocate to Agency B's facility, the ____contact listed below will be notified by phone or other available system of communication of Agency A's intent to relocate.

c. Both parties agree to work with a strong spirit of cooperation and mutual regard for each other's critical mission. Jasper School District personnel will only remain at __Agency B's facility until Jasper School District secures another location through Arkansas Building Authority.

d. Jasper School District will also pay pro-rated reimbursement for utilities, maintenance, janitorial, and fuel costs, for the time the Agency B's facility is occupied.

3. POINTS OF CONTACT

Agency	Contact Name	Phone

4. This MOU is implemented as of the date of the last signature and will remain valid by mutual agreement of the parties.

5. SIGNATURES

_________________________________ _______________________
Name Date
Director Jasper School District

_________________________________ _______________________
Name Date

Director Agency B