Missouri Center for Education Safety v1.4 (updated 3-30-2016)

Information Technology (IT)/Cyber Security Checklist

Disclaimer: *The following checklist has been developed by the Missouri Center for Education Safety, through a review of established and recognized guidelines and other resources related to cyber security, and in consultation with the Federal Bureau of Investigation, US Department of Homeland Security, Missouri Office of Administration, and the Office of the Missouri State Auditor. Due diligence has been performed to develop a comprehensive and relevant resource for Missouri schools to use, to insure they are providing adequate consideration to sensitive information and data protected by numerous federal, state, and local laws and regulations. No expressed or implied warranties or guarantees are provided as to the accuracy or adequacy of this checklist. Every fact or interpretation can change a recommendation. This checklist is not offered to support or in lieu of legal advice. The school district is responsible to seek legal and administrative advice before implementing any measures or recommendation referenced in this checklist.*

Areas of Consideration

1. Data Governance:

The district has established a comprehensive data governance program to assure the data management and protection procedures in place are effective in reducing data privacy and security risks due to unauthorized access or misuse of data. y/n

Without a formal data governance program, the district cannot ensure that PII maintained by the district is adequately protected and safe from unauthorized access, misuse, or inadvertent disclosure. Establishing a data governance program is a critical task for any educational organization. An effective program requires establishing decision-making authority, defining policies and practices for the protection of sensitive data, identifying and gaining support of stakeholders, implementing the program, and monitoring its success. By clearly establishing policies, standard procedures, responsibilities, and controls for data activities, a data governance program helps to ensure that information is collected, maintained, used, and disseminated in a manner that protects privacy, confidentiality, and security, while allowing educational organizations to meet their missions. The district should establish and implement a formal data governance program encompassing the full life cycle of data, from acquisition to use to disposal.

Data Governance focus areas include but are not limited to:

- *The district should formally assign and document responsibility for management of the district's data.*
- *The district should develop and document a formalized data stewardship plan which clearly documents policies and procedures to protect student data. Adopting and enforcing clear policies and procedures in a written data stewardship plan is necessary to ensure that everyone in the organization understands the importance of data quality and security, and that staff are motivated and empowered to implement data governance.*
- *The district should maintain an inventory of data files, data elements maintained in those files, and the criticality or sensitivity of the data. Conducting an inventory of all data that*

require protection is a critical step for data security projects. Maintaining an up-to-date inventory of all sensitive records and data systems, including those used to store and process data, enables the organization to target its data security and management efforts.

- *Classifying data by level of sensitivity helps the data management team recognize where to focus security efforts.*
- *The district should formally identify and document the source and content of elements within the data files maintained by the district. Closely managing data content, including identifying the purposes for which data are collected, is necessary to justify the collection of sensitive data, optimize data management processes, and ensure compliance with federal, state, and local regulations.*
- *The district should implement and document a monitoring process to detect unauthorized disclosures of PII within its custody. Ensuring the security of sensitive and personally identifiable data and mitigating the risks of unauthorized disclosure of these data is a top priority for an effective data governance program. (see also PII/FERPA related suggestions under "General IT Security" below)*
- *The district should adopted and document a formal policy regarding the archival or destruction of data at the end of its lifecycle. While some data may need to be maintained indefinitely according to various laws and regulations, other data may become unnecessary or irrelevant when a student graduates or otherwise leaves the district, and can be destroyed when no longer needed. Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records). Establishing policies and procedures governing the archival or destruction of data allows an organization to more efficiently and safely protect its data and is a critical component of an effective data governance program.*

2. Security Awareness Program:

The district has established a formal security and privacy awareness training program. y/n

According to accepted standards, the purpose of computer security awareness, training, and education is to:

(1) enhance security by improving awareness of the need to protect system resources and developing skills and knowledge so computer users can perform their jobs more securely; and

(2) build in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems. Additionally, guidance from the U.S. Department of Education, PTAC encourages organizations to provide security training on a recurring basis, communicate privacy policies to users, and define a process for reporting privacy incidents and complaints.

Making computer system users aware of their security responsibilities and teaching them correct practices helps users change their behavior. Awareness training also supports individual accountability, which is one of the most important ways to improve computer security. With proper security and privacy awareness training and clear communication of data and device use policies, employees can become the first line of defense against cybersecurity incidents.

However, without adequate training, users may not understand system security risks and their role in implementing related policies and controls to mitigate those risks.

3. **Security Controls:**

The district implemented all necessary security controls, to insure district technology assets, including PII, at risk of inappropriate access, use, and disclosure, are properly protected? y/n

The district has formally appointed and documented the responsibility for specific personnel to serve as security administrator(s) or formally assigned responsibility for creating, implementing, and maintaining security policies and procedures. y/n

Accepted guidance from the U.S. Department of Education, PTAC states that organizations should develop comprehensive plans outlining organization policies and standards regarding data security and individual privacy protection. Such plans should clearly identify staff responsibilities for maintaining data security and empower employees by providing tools they can use to minimize the risks of unauthorized access to PII.
The district's information technology director and assistant information technology director should formally be tasked with maintaining the security of the district's technology resources and data. A formal designation of staff responsible for security administration, helps to insure that the risk that security policies and procedures are adequately designed, documented, implemented, and updated.

4. Access Control:

The district has fully established policies and procedures regarding user access to systems and data. y/n

The district IT systems display logon banners to users accessing district systems and data. y/n

Logon banners should display information to system users regarding applicable privacy and security notices and required compliance with applicable laws, regulations, and policies. According to accepted standards, logon banners should state that a user is accessing a district provided information system; that usage of the system may be monitored, recorded, and subject to audit; that unauthorized use of the system is prohibited and may be subject to criminal and civil penalties; and that use of the system constitutes agreement with the terms. Without a displayed logon banner, users may not be informed or aware of the authorized or appropriate use of the system and data, and any criminal prosecution related to intentional data breaches may be complicated by this lack of notice.

5. Concurrent User Controls:

The district has established controls to restrict concurrent access to district systems. y/n

Concurrent session controls prevent a single user from accessing an information system from more than a specified number of locations at any given time. These controls help prevent unauthorized users from accessing the system by masquerading as an authorized user. According to accepted standards, the number of concurrent sessions for a user should be limited. Without limiting access from multiple locations at the same time, management may not be able to ensure the confidentiality, integrity, and availability of data and the system.

6. Security Logs:

The district has formally documented policies and procedures to identify the types of security events to be logged and monitored. y/n

Without an effective method to identify, log, and monitor significant security-relevant events, the district is at increased risk that unauthorized or inappropriate system activity may not be detected. The internal security policies within a district's network management system, using default logging settings, can log thousands of entries each day. A majority of these entries, such as notification of successful login by system users, are of minimal use for security purposes. The security logs are voluminous and cannot effectively be monitored for unusual or suspicious activity.

The district should establish relevant criteria and identify significant system events that should be logged, and the logging settings customized. At a minimum, all such significant events, including access to and modification of sensitive or critical system resources, should be logged. Also, logging should include appropriate information to facilitate monitoring of such significant system events.

7. Physical Security for IT Assets and Systems:

The district has fully established physical security controls to ensure protection of technology resources. y/n

All IT/Cyber assets are inventoried and policy in place to periodically check the inventory list against actual inventory.. y/n

Policy in place re taking and using school IT assets home, off site, etc. y/n

Policy in place re personal IT assets to include computers, tablets, and smart phone/devices being brought onto school property and being allowed to access school network, etc. y/n

Policy covers securing data storage/server rooms to prevent unauthorized access by students, visitors, employees who don’t legitimate need for access to these rooms. y/n

Responsibility for physical security of technology resources should be formally assigned and documented. y/n

A documented policy for physical access to technology resources, including who can be authorized access to restricted or sensitive areas, should be established. y/n

Keys to access restricted areas should be controlled and spare key access should be properly monitored and documented. y/n

Annual briefing/training of all staff on cyber/IT rules and policies. y/n Date of last briefing/training:______________

8. Virus/Trojan/Malware, etc:

A formal process in place and documented to insure current anti-virus and firewall programs installed on school computer and updated on a regular schedule. y/n

Anti-virus programs are implemented and configured to check every file that gets to computers (e.g., disks, cd-rom, email and the web) . y/n

Updates for software patches are regularly checked and installed to reduce system vulnerability and log maintained of those updates. y/n

9. Back-Ups:

Back-ups conducted on a schedule, on appropriate media, and stored off site in a secure manner, in an encrypted format. y/n

The back-ups are “air gapped” and not accessible remotely in any manner or fashion. y/n

10. Passwords:

Accepted password policy in place, requiring strong passwords with regular changes to the password, documented policy against sharing of passwords, maintaining passwords in a secure manner, etc. y/n

This should include identifying and documenting policies for the following:

- *Resetting lost or compromised passwords.*
- *Policies regarding which security groups system users may be assigned to, along with the access rights granted each group.*
- *Policies describing who may be granted privileged access to district systems.*
- *Notifying security administrators of the need to disable accounts for users terminating employment.*

11. Data Breach:

Data breach response policy, approved by the organization's leadership, which is germane to its environment. y/n

Plan in place to document and respond to data breaches and to mitigate any such breach of "Personal Identifying Information" (PII). y/n

Employee roles are pre-identified in the plan, and each employee understands and is familiar with those roles, and has received appropriate training, participated in drills, etc . y/n

A data breach drill/exercise has been conducted to test staff, systems, etc. y/n Date of last drill or exercise:____________________

Contact phone numbers for law enforcement, vendors, etc. are current and up to date. y/n Date the contact list last updated:_________________

Networks mapped and drawn so that school IT staff can show an outside investigator detail of the system and logical investigative avenues to pursue. y/n

Critical infrastructure points noted with directions on how to proceed if data in these points has been compromised (your "personal identifying information" (PII). y/n

Potential sources of evidence identified (logs from IDS, routers, etc.) and everything in a comprehensive package so that when things do go bad, staff will be prepared and critical information is in one location that will help guide the response to the data breach. y/n

Response plans practiced on a regular basis. y/n

12. Inactive Account Monitoring:

The district proactively monitors for user accounts that have not been accessed or used for a specified period of time. y/n

Without appropriate account access policies and procedures, users may be granted inappropriate or unauthorized access, which can provide opportunities for misuse or inappropriate disclosure of sensitive data. Inactive accounts can indicate users no longer need the access privileges provided by the accounts and may be attractive targets for individuals attempting to gain unauthorized access since the account owners may not notice illicit activity on the accounts, according to the GAO. Without appropriate monitoring, security administrators are less likely to identify user accounts that had not been accessed or used for a specified period of time.

13. User Access:

The district performs periodic reviews of users' access to data to ensure access remains appropriate and aligned with job duties. y/n

The district has established and documented formal policies and procedures, including requiring standard forms, for requesting, approving, and maintaining access to systems. y/n

The district periodically monitors user account access to identify and evaluate inactive accounts. y/n

The district periodically review user access to data and other information resources to ensure access rights remain appropriate and are commensurate with job duties and responsibilities. y/n

As users' work assignments and job responsibilities change, access rights to district systems may be added, changed, or removed. Over time, users can accumulate access rights that are no longer necessary, increasing the risk of inappropriate access to district data. Without periodically reviewing user access rights, there is an increased risk that unauthorized alterations of the rights will go undetected or that access rights may not be aligned with current job duties.

14. Continuity Planning:

The district has documented and tested a complete continuity plan. y/n

Individuals responsible for carrying out those duties have received formal training. y/n

Elements of a continuity plan the district has been documented and include:

- Priorities and procedures for the restoration of critical systems and data. y/n
- Identification of persons responsible for restoration of specific systems and data. y/n
- Formal identification of the resources and data included in the district's backups. y/n

A comprehensive test of backups to ensure that data can be successfully recovered in the event of a disaster has been performed. y/n

According to accepted standards, a continuity plan or suite of related plans should be developed for restoring critical business functions and applications. The plans should include arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. Staff should be trained and aware of their responsibilities to prevent, mitigate, and respond to emergency situations. For example, information security support staff should receive periodic training in emergency fire, water, and alarm incident procedures; and specific responsibilities for initiating and running an alternate data processing site.

Additionally, testing continuity plans is essential for determining whether the plans will function as intended in an emergency situation. The most useful scenarios involve simulating a disaster situation to test overall service continuity. Such an event would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation. Any testing of a continuity plan is likely to identify weaknesses in the plan, and it is important the plan and related supporting activities, such as training, be revised to address these weaknesses. Otherwise, the benefits of the testing will be mostly lost.

Without a tested and functional continuity plan, management has limited assurance the organization's business functions and computer processing can be sustained during or promptly resumed after a disruptive incident.

The district should:

- *Establish and document an incident response plan that includes centrally tracking all security incidents.*
- *Formally document and adopt a comprehensive data breach response policy to promote an appropriate response in the event of a breach of protected student data.*
- *Develop a comprehensive continuity plan and formally assign responsibilities for development, implementation, and maintenance of the plan to appropriate personnel. Once established, ensure the plan is tested on a periodic basis.*

15. Vendor Monitoring:

The district has established a process for ensuring software acquired or outsourced from information technology vendors complies with accepted data security principles. y./n

Copies of vendor contracts should be maintained in a secure location, and periodically reviewed to insure emerging best-practice security policies and practices are incorporated into the contracts. Contract language should include a clause stating the vendor will provide appropriate security functionality for the district. District staff should periodically ask vendors to provide documentation that their product's security functionality meets generally accepted industry standards.

The district should develop procedures to formally monitor information technology vendors to ensure the district's data is properly protected and the vendor acts in accordance with contract terms and conditions.

16. General IT Security:

The following are general IT security guidelines, and may already be addressed, in part, in the above sections, but are set out below to insure all security aspects of the district's IT program have been reviewed and documented.

Identification of PII/FERPA and other sensitive information maintained by organization is known and documented, where it is stored (including backup storage and archived data), and how it is kept secure. y/n

All staff are familiar with PII/FERPA requirements re protection of student information through training and briefings, and documented. y/n

E-mail communications which contain PII/FERPA protected information is encrypted during transmission and protected from unauthorized disclosure at all times. y/.n

Regular risk assessments are conducted and privacy threats for organization, as well as any contractors, vendors, and other business partners are evaluated. y/n

Periodic review of who is approved for access to PII and/or other sensitive information and checking user activity status to determine if accounts are inactive and should be deactivated after a pre-determined period of inactivity. y/n

Separation of duties relative to cyber security to help ensure integrity of security checks and balances. y/n

Mitigation controls are in place designed to prevent and detect unauthorized access, theft, or misuse of PII and/or other sensitive data. y/n

Security controls, such as encryption of sensitive data in motion and at rest (where feasible) are implemented. y/n

Data destruction policies are in place and periodically reviewed to minimize the risk of data breaches through unauthorized access to archived media or computers that are no longer in use. y/n

Frequent privacy and security awareness trainings are conducted as part of an on-going training and awareness program. y/n

Mandatory privacy and information security training is provided on a recurring basis to all employees, school officials, contractors, and any other staff involved in data-related activities. y/n

Privacy policies are posted and communicated to customers and users (for instance, on the agency web page or on a bulletin board at the office, through statements inserted in documents or emails, etc). y/n

Processes for reporting privacy incidents and complaints is clearly defined and easily reported. y/n

17. Additional Notes:

- While FERPA itself does not contain specific breach notification requirements, it protects the confidentiality of education records by requiring recordation of each incidence of data disclosure.
- As stated in the preamble of the 2008 amendment to the FERPA regulations: “The U.S. Department of Education does not have the authority under FERPA to require that agencies or institutions issue a direct notice to a parent or student upon an unauthorized disclosure of education records. FERPA only requires that the agency or institution record the disclosure so that a parent or student will become aware of the disclosure during an inspection of the student’s education record. … FERPA does not require an educational agency or institution to notify students that information from their education

records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR 99.32(a)(1). In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft" (Family Educational Rights and Privacy, Final Rule, 73 Federal Register 74843-74844 [December 9, 2008]).

18. References:

Additional IT/Cyber Security information can be found at:

- US Department of Education, Privacy Technical Assistance Center (http://ptac.ed.gov/)
- US Computer Emergency Readiness Team (https://www.us-cert.gov/ccubedvp)
- National Cyber Security Alliance (https://www.staysafeonline.org/)
- Missouri State Auditor Report Number 2016-015 (http://auditor/mo.gov)