Missouri Center for Education Safety v1.3

Information Technology (IT)/Cyber Security Checklist

Virus/Trojan/Malware, etc.

Current anti-virus and firewall programs installed on school computer and updated on a regular schedule. y/n

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

Software patches regularly checked and installed to reduce system vulnerability and log maintained of updates. y/n

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

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

Physical Security

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

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. y/n

Contact phone numbers to for law enforcement, vendors, etc. are current and up to date. y/n

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

General IT Security:

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

Note:

- 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]).
- 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/)