SCHOOL DISTRICT POLICY GUIDELINES

FOR THE COLLECTION, ACCESS, PRIVACY, SECURITY AND USE OF STUDENT DATA

In the 2017 Legislative Session legislators amended W.S. 21-2-202 (a)(xxxvii) (A-E) to require the Wyoming Department of Education in consultation with the Department of Enterprise Technology Services, the Department of Audit and school districts, to establish and maintain guidelines for school districts for the collection, access, privacy, security and use of student data by school districts. The guidelines shall, at a minimum, be in compliance with the federal Family Educational Rights and Privacy Act and other relevant federal and state laws.

W.S. 21-3-110 (a)(xxxv) requires districts to write their own data and security policies and have them adopted by the district board of trustees and effective no later than January 1, 2018 using the guidelines established under W.S. 21-2-202(a)(xxxvii).

Below are some guidelines based on industry standards and best practices for you to consider as you draft your district data security and privacy policies. Guidelines are a general rule, principle, or piece of advice. It is recommended you have a conversation with your stakeholders and adopt policies most relevant to your district.

DATA COLLECTION

- Districts may want to consider posting a list of student level data elements on their public website for transparency purposes.
- Eliminate collection of Social Security Numbers (SSN) whenever possible.
- Collect only the minimum amount of personal information necessary to achieve your purposes and collect only that which you are authorized.
- Consistent data entry procedures in all applications. For example require that legal names be used in all software. Maintaining strict input validation on form fields will help ensure data validity.
- Never email student data in a clear text or unencrypted email.
- When providing data through FTP, ensure Secure File Transfer Protocol (SFTP) is used.
- Always use a secure connection from online data systems such as PowerSchool and Infinite Campus.
    - Online access to confidential data should be done using a secure web connection SSL/TLS or HTTPS:

AUTHORIZATION AND AUTHENTICATION MECHANISMS FOR ACCESSING STUDENT DATA

PASSWORDS

- Employees should not share their passwords with anyone (including peers and supervisors).
- Often times, passwords can be compromised when you have them written down.

- It is always a good idea to use strong passwords that are not predictable. Strong passwords are usually at least 6 or more characters in length and are a combination of letters, numbers and symbols (@, #, $, %, etc.). Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase.
- Districts should have a password change policy that requires employees to change passwords regularly. Passwords should not be repeated (re-used) and users should not use the "save, store or remember password" feature in the application or browser.
- Establish an account lockout policy to limit the number of consecutive failed login attempts due to a bad password.
- System administrators and super users should have higher security settings for their passwords.

PERMISSIONS

- Only use the local administrator account when necessary to install or update software.
- Have a procedure to edit or modify permissions as employees change positions or roles and disable accounts for exiting employees so that sensitive data is no longer accessible.
- The "Principle of Least Privilege" (POLP) is a best practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the POLP translates to giving people the lowest level of user rights that they can have and still do their jobs. This applies to contractors as well as district employees.

SESSION MANAGEMENT

- Web applications should provide mechanisms that allow users to actively close their session once they have finished using the web application.
- Automatic session expiration should be used whenever possible. All sessions should implement an idle or inactivity timeout.
- Absolute timeout should be used regardless of session activity.
- The session expiration timeout values must be set accordingly with the purpose and nature of the web application, and balance security and usability, so that the user can comfortably complete the operations within the web application without his session frequently expiring. Both the idle and absolute timeout values are highly dependent on how critical the web application and its data are.

ADMINISTRATIVE, PHYSICAL, AND LOGICAL SECURITY SAFEGUARDS, INCLUDING EMPLOYEE TRAINING AND DATA ENCRYPTION

ADMINISTRATIVE SECURITY

- Have written policies governing access to, duplication and dissemination of all electronic confidential information or Personally Identifiable Information (PII). Have written procedures for employee hiring and termination. Establish procedures for access and handling of data for volunteers and student office assistants.
- Employee confidentiality agreements should be signed and the process documented. How do you enforce signing of confidentiality agreements by employees?
- Internal auditing and monitoring procedures should be documented. Do you monitor for login attempts and failures? Do you monitor social networks? Do you check to see what users are doing on your network?

- Monitor activities and procedures of third-party contractors with access to your computer systems and network.
- Written agreements should be in place with third-party contractors before they begin work. Written agreements need to cover access to, duplication, and dissemination of confidential information; physical and logical security, and contract termination procedures.
- Conduct appropriate background checks on employees, volunteers, contractors and vendors in accordance with policy, procedure and any applicable law. Have a well-organized, well understood, well-maintained, and well-monitored security policy for both internal and external users, and ensure they have refresher training.
- Create and maintain a network flow diagram for all current hardware and infrastructure networks and a data flow diagram for all information systems.
- Coordinate with your HR office to develop an "exit strategy" for terminated employees to remove their access to district systems and ensure any physical devices are accounted for.
- Governance - Senior administrators must approve the district's Information Security program and policies.

PHYSICAL SECURITY

- Never leave sensitive data on your desk, in unlocked cabinets, written on whiteboards or paper.
  If your computer is in a public area make sure computer screens are not in plain view or utilize a computer screen privacy filter.
  Appropriately destroying sensitive data when no longer needed is a must. This is both for stored and any printed sensitive data.
- Computer screens that are left unlocked and unattended allow for unauthorized access. Manually locking your workstation or leveraging automated screen lock functionality can help deter and prevent unauthorized access.
- Wipe computer hard drives or properly destroy them as staff exit and computers and other devices are retired to ensure that sensitive data is properly destroyed; consider writing over the free space with other data to prevent recovery.
  - **NIST Guidelines for Media Sanitation**
- Server rooms should be dry and temperature controlled. Be aware of utility and water lines that run over or near the server rooms that could malfunction, leak, or allow unauthorized access into the server area.
- Ensure UPS battery backups are installed and the batteries are checked regularly.
- Make sure all hardware and software is covered by a service agreement and is phased out before it is no longer supported.
- Lock your server room and restrict access to only technology related staff. Key card/key fob access with logging and monitoring capability is best. Routinely review the logs. Video surveillance may be helpful as well.

LOGICAL SECURITY

- User account management procedures should include the following:
  - Timelines for user account deactivation should be set up for vendors or contracted staff with a known end date.
  - Ensure that user accounts are reviewed regularly or after job changes such as transfer, promotion, etc.
  - Unique accounts requiring individuals to be linked to the accounts and actions

- Firewalls
    - Firewall or comparable security appliance rules should be reviewed at least every six months whether the district or a third party maintains the firewall.
    - Employ logging strategies for networked devices.
        - Develop consistent processes for reviewing logs and tracking incidents based on your district's needs
- Remote access
    - Which users will be allowed to access the network through a VPN?
        - Consult with your HR office on policies for telecommuting or work from home.
    - What level of access should be given to each type of user?
    - Develop guidelines for which devices to allow to connect to the network through a VPN.
    - Which authentication method will be used?
    - Develop session management guidelines including idle timeout and absolute timeout.
- Consider disabling any unused network ports or protocols and also consider disabling unused physical ports on network equipment.
- Enable intrusion detection and access controls on the wireless networks.
- Utilize two-factor authentication if possible, requiring extra information or a physical device to log in, in addition to your password.
- Removable media devices can contribute to security breaches coming into or leaving your network. Develop a policy regarding the use of USB drives, external hard disks, thumb drives, external DVD writers, and any other writeable media. Ensure devices are encrypted before issuing to staff and instruct staff not to use personal devices for storing or transporting PII or other related school district information.
- Mobile Device Management
    - Never leave your mobile device unattended in public places.
    - Enable auto-lock and password protection or biometric protection.
    - Disable wireless access such as Bluetooth or Wi-Fi when not in use to prevent unauthorized access.

      You can help protect your company's information on your employee's company-issued mobile devices, preferably with the ability to remote lock and remote wipe lost or stolen devices. Some products come with this functionality built-in.
    - Encrypt laptops so in the event that they are lost or stolen they cannot be accessed.
    - Make sure all operating systems and applications are patched and updated regularly.
    - Do not allow staff to take district devices out of the country.
- System updates and antivirus software are important tools to keep data protected. It is very important this software and all computers and devices receive regular software and signature updates.
- Database systems guidelines:
    - Set data standards that keep into account authority guidelines such as FERPA.
    - Make sure database software is up to date
    - Only appropriate personnel should have access to databases
    - Limit ownership of data to users who absolutely need the rights (consider POLP)
    - Districts should verify that all data falls under appropriate data classifications
    - Assign data owners to the database and the data owners assign security
    - District should involve business owners in defining data classification
    - Base data and systems security on the classification levels of the data
    - Vulnerability scans should be done against your organization's databases. There are both private and open source solutions that districts can use to address this. For more information see **SANS guidelines**.

EMPLOYEE TRAINING

- Ensure that your data and security policies are easily accessible by all employees and that you have a procedure for sharing them with newly hired staff.
- Provide recurring technology and data security best practices training for all employees.
- It's not enough to simply tell your staff not to use their work devices for non-work related activities. You can help protect citizen data by developing a written policy and have users sign and acknowledge they have read it. The policy should be designed with a balance in keeping the user productive and won't become outdated as your office grows.
- Malicious attackers are working hard to steal information and many of these attempts come to you through your email or while visiting websites. Employee Training should be regularly conducted and include:
  + Avoid opening any email or email attachments from unknown or suspicious sources or that look significantly different from email you typically receive from a known associate.
    - Phishing is defined as: the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
  + Do not share your password credentials with anyone or enter them into suspicious websites. Often sites will duplicate the original and look identical. When in doubt, find the original website and log in there instead of using a link sent to you.
  + Avoid clicking on any links in websites that appear suspicious.
- Consider using a commercially available training course that includes videos.

DATA ENCRYPTION

- Confidential data in transit:
  + Data transmitted by a third party through an interface to another system, domain or enclave will be done securely using known secure protocols such as TLS/SSL, sFTP or other agreed upon methods.
- Confidential data at rest:
  + Data will be stored securely at rest using AES 256 or stronger or another acceptable standard.
- Student data will not be transmitted over email unless secured using cryptographically strong email encryption tools such as PGP or S/MIME or another acceptable standard.

PRIVACY AND SECURITY COMPLIANCE

DATA PRIVACY COMPLIANCE

- Chances are most of your staff are regulated by FERPA. You should ensure that your staff are familiar with the appropriate data privacy laws and regulations and ensure they are enforced.
- Refresher trainings in FERPA regulations should be offered at regular intervals. The **Privacy Technical Assistance Center (PTAC) website**, has a FERPA 101: For Local Education Agencies video.

USE OF STUDENT DATA

- Never email student data in a clear text or unencrypted email.
- Ensure all users of student data have a legitimate educational interest prior to allowing use.
- Do not release student data to law enforcement without a signed judicial order or warrant.

EXCEPTION STANDARDS

A standardized exceptions process will allow a district to document security requirements that affect the district's business needs. The process document will discuss associated risk and will document alternative solutions. Information Technology Directors and administrators will review the exception request and make the final decisions. If the exception standard is approved the period of the exception should be limited (example one year) and follow up should be performed to ensure the exception is still valid.

CONTRACTS AND DATA SHARING AGREEMENTS

FERPA requires the educational agency or institution execute a written agreement when disclosing personally identifiable information (PII) from education records without consent. The mandatory elements of the written agreements vary slightly depending on whether the agreement is for a research study or an audit/evaluation. Best practice checklists can be found **here**.

RISK ASSESSMENT

- Level of risk is often a key factor in many IT decisions. It is always a good idea to conduct an annual risk assessment on applications and key IT infrastructure (Self and/or 3rd party). Minimum criteria for an effective risk assessment includes:
  + Knowing what information security assets you have.
  + Knowing what value those assets have to the organization.
  + Knowing what vulnerabilities exist in your assets.
  + Knowing what threats exist to your assets.
  + Threats to confidentiality, availability, and integrity must be considered.
  + Knowing the likelihood that one of the vulnerabilities will be attacked by one of the threats.
  + Knowing the potential business impact of a successful attack.
  + Knowing how to recover from an incident or attack.
- Consider utilizing monitoring tools and vulnerability scanning tools to help identify system weaknesses.
  + Scan systems regularly and notify business owners of the results.
- Assign data owners to data assets such as financial and student data. Data owners should not be information technology personnel.
- Actively document fixes to any network changes that correct weaknesses.

CHANGE MANAGEMENT

- Document a change management process for software, hardware, and personnel changes.
- Establish a change management board.

WORKSTATION SECURITY

- Have a standard security configuration for all workstations software settings.
- Host based firewall should be active for all networked workstations.
- Document and implement who is authorized to use the workstations.

PROCESSES FOR IDENTIFICATION OF AND RESPONSE TO DATA SECURITY INCIDENTS, INCLUDING BREACH NOTIFICATION AND MITIGATION PROCEDURES

- Devise and regularly test your security incident response plan.
- Your district may want to pay for a phishing simulator to send fake emails to your staff as a training tool.
- Maintain contact lists of designated Incident Response Team members.
- Plan for reporting and notification of incidents.

MALICIOUS DATA BREACH

What procedures do you want your staff to follow in the following events?

- Theft of a Laptop or Computer.
- Breach of your computer network via a malicious email.

NON-MALICIOUS DATA BREACH

What procedures do you want your staff to follow in the following events?

- Loss of a thumb drive or laptop.
- Loss of a paper document with student information.

STANDARDS FOR RETENTION AND VERIFIED DESTRUCTION OF STUDENT DATA

Paper records are governed by existing Wyoming records retention schedules outlined in W.S. 9-2-405 through 9-2-413.

Create an electronic record retention schedule that takes into consideration:

- How long will you need student data for audit purposes?
- Can student level data be aggregated for long term data analysis?
- If student data is necessary for long term data analysis can student names be eliminated from data files?

BACKUP AND DISASTER RECOVERY

If a disaster strikes in any form, having a backup is crucial. It is always a good idea to make regular backups of your data and keep copies in a secure offsite location. This includes email servers where applicable.

Regularly test restoring your data from your backup. Often times there may be issues preventing you from successfully recovering your data. Testing recovery may reveal faults in your disaster recovery plan, rather than having them surface during a critical need to restore.

Ensure backups are protected by the same standard of physical and logical security as operational systems. Develop a written backup recovery plan and review it periodically.

LINKS TO HELPFUL RESOURCES

- **WDE Data Governance**
- **Wyoming Department of Enterprise Technology Services**
- **National Institute of Standards and Technology**
- **National Cybersecurity Alliance**

WYOMING
DEPARTMENT OF EDUCATION