Data Security

TOM ACKERSON - WASATCH SCHOOL DISTRICT

Have a Plan

- The plan needs to be dynamic in nature and available to staff.
- Training, training, training always training.
  - incorporate items from the plan into meetings –
- Good security policy protects not only the district, but all users.
- Helps you to comply with all state and federal laws.
- A plan will help you educate your data stewards – technical or non-technical

Security and Confidentiality

- Understand what you are protecting

  "The district makes every effort to abide by all applicable State and Federal guidelines, policies, regulations, statutes, and procedures pertaining to the confidentiality and privacy or data." *from the policy manual-*

- Get an understanding of FERPA

  "FERPA assures students that their records are protected from unauthorized access or disclosure and requires a clear understanding of the type of information that can be released without an individual's consent." *from the policy manual-*

- Look at the guide and make sure policy reflects it

  http://nces.ed.gov/pubs2006/2006805.pdf

Individual Employee Rules

- Define <u>who</u> gets to see <u>what</u>

  "Employees will access only data that are required for their job." *from the policy manual-*

- Make them aware of how, where, and when they can use data

  "Employees will maintain the security of all WCSD data in their possession or to which they have access by protecting computer media, forms and printouts from unauthorized access and will dispose them in a safe manner." *from the policy manual-*

- Access to student data should be handled with good policy

  Avoid uncomfortable or confrontational show-downs to data access. Make the decisions on who gets what access well ahead of them requesting it. If you have good guidelines, the decisions are easier for all to abide with.

Send and Receive Securely

- Avoid email

  "Staff is never to send sensitive information as e-mail. If e-mail absolutely must be used, the file is to be encrypted and sent an attachment rather than in the text of the e-mail message." *from the policy manual-*

- Setup for secure transfers

  "Secure FTP and SSL are always to be employed when transmitting data to and from district facing applications." *from the policy manual-*

  Setup your own secure FTP sites, password authenticated file sites, and secure areas for data transmission and reception. Never use "consumer" sites that you have no authority over.

Store and Monitor Securely

- Limit access to you sensitive information

  "Never store sensitive data/information in such a way that it co-mingles with other data on disks or other removable data storage media. " *from the policy manual-*

  Take a look at the student data that is being stored in Excel and other spreadsheet type programs. Are you protecting that data as thoroughly as your secure SQL server?

- Monitor the activity of your secure storage

  Setup logs and have monitoring in place to determine how files have been accessed and used.

- Secure your backups

  "Backup files require the same levels of security as do the master files " *from the policy manual-*

Data Access Security

- Most security problems are a result of human error

  "By instituting security procedures, the organization protects not only the system and its information, but also each user who could at some point unintentionally damage a valued file." *from the policy manual-*

- Passwords

  Have users change passwords. After an independent audit of many district passwords it has been recommended that these actions be taken to improve security. The majority of the old passwords in the password database were cracked within 3 seconds.

Network Security

- Protect your network both physically and virtually

  “An "access node" is a point on a network through which you can access the system. If even one such point is left unsecured, then the entire system is at risk.” *from the policy manual-*

- Secure wireless

  Have a different wireless access for your sensitive information. Make sure that guest access is adequately partitioned from your data network.

- USB Drives

  “Special care must also be taken when placing data of any sort, especially confidential data on a USB due to ease by which they can be lost or misplaced. In general, USBs should be avoided as a means of moving any type of sensitive data even if encrypted..” *from the policy manual-*

Acceptable Use Policy

- All users need to sign a policy

  "Signed and filed agreements verify that users have been informed of their responsibilities and understand that they will be held accountable for their actions." *from the policy manual-*

  Users need to know what is acceptable and what is not.

- New employees

  "Once hired, new employees should be informed of, and trained on, acceptable use and security policies as a part of their initial orientation in order to impress the importance of security upon them." *from the policy manual-*

Train, Train, Train

- Train staff to meet the specific security responsibilities of their positions
- Inform them that they are monitored
- Remind them that breaches in security carry consequences

  "Assure staff that reporting potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making)." *from the policy manual-*

  Make them your "Data Security Helpers" not your enemy
- Review policies with staff every chance you get

  Raise staff awareness at every level of your organization. Let them raise questions in an open forum or setting and then you can clarify policy and work through ways to gain support and compliance for policy.

Last But Not Least…
Have a Data Breech Plan

- Make a data breech possibility part of your written plan
- Hard drives fail, so can the best laid security plans
- Know what your exposure is before an incident
- Have a Data Breech Checklist ready

  http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

Data Security

THANK YOU