SHAWNEE MISSION SCHOOL DISTRICT

DATA COLLECTION, STORAGE, AND TRANSMISSION SECURITY

Presented to the House Education Committee
February 12, 2015

- In the performance of its regular business operations, the Shawnee Mission School District collects, stores, and transmits sensitive student and personnel data as required by the state and federal government.

- The board of education, administrators, and staff, many of whom are also parents and taxpayers, take these issues very seriously. We retain medical data on students only as necessary related to the safety, security, and well-being of students. This necessary data includes immunization records, known allergies, and/or other data that parents impart to us.

- Data security is a foundational component of all collection, storage, and transmission activities during the entire lifecycle of the data.

- The Shawnee Mission School District complies with applicable state and federal statutes.
  - Family Educational Rights and Privacy Act (FERPA)
  - The Protection of Pupil Rights Amendment (PPRA)
  - Children's Online Privacy Protection Act (COPPA)
  - KSA 72-6215 through 6223 (Student Data Privacy Act), a.k.a. Senate Bill 367 (2014)
- The Shawnee Mission School District follows best practice for collection, storage, and transmission of data.
  - National Institute of Standards and Technology (NIST) Special 800 Publications
  - Payment Card Industry (PCI) Data Security Standard (DSS)

- Security controls are applied in layers and at critical junctions across the many networks, systems, and cloud-based services in use.

    - Physical access
    - Account management
    - Secured networks
    - Secured systems
        - Software management
            - Regular updates
            - Patch management
    - Secured transmissions
    - Audit review, analysis, and reporting
    - Management of end- of-life data

- The people that use systems and transmit data are a critical component of a solid security stance. The district recognizes the importance of engaging people to educate them about best practice and helping them maintain a security-conscious mindset.

  - Regularly reviewing, developing, and adapting the district's security stance
  - Employment of CISSP for on-site data security expertise
  - Research and education by engaging third-party experts
  - Coaching personnel on avoiding social engineering

- Parents and patrons should be aware of the information the district collects, stores, and transmits. They should also be aware of the district's obligation and commitment to keep sensitive data private and confidential.

  - Public notices published annually in paper of record
  - Public notices via district's web page
  - Communication mechanism in place to alert patrons about breaches