



OLATHE PUBLIC SCHOOLS USD 233

Students Prepared for *Their* Future

OLATHE PUBLIC SCHOOLS NETWORK AND DATA SECURITY

Presented February 12th, 2015
House Education Committee

Olathe Public Schools Technology Division is dedicated to providing staff and students a technology environment to prepare our students for their future in the global workplace.

Safety and security of the network and all data which resides there is a primary focus.

- Core Network Security Components
 - Firewall to prevent unauthorized access
 - Intrusion Prevention Systems monitors traffic through the firewall and provides a second layer of security
 - Security Event Managers for comprehensive analysis and reporting
 - Hardware Security including anti-virus protection, operating system updates, refresh of aged equipment
 - Web Filters to block inappropriate content and provide first line of defense to malicious web sites

- Core Network Security (cont.)
 - Anti-Virus Protection using enterprise virus/malware/spyware applications
 - Network monitoring systems to report uptime, outages, potential trouble
 - Physical security to all data centers using keyless or keyed systems including security cameras at the core data center
 - End-of-life procedures on destruction of hardware and digital media according to NAID (National Association of Information Destruction) and NIST (National Institute of Information Destruction) standards

- Data Security
 - Account Management requiring strong passwords, forced password changes, limited access attempts, user authentication
 - Device management to restrict attachment of devices to the network to known/owned devices, strictly limited remote access from outside the network, auto shut-down of devices nightly
 - Role based secured authorization to student, employee, financial and administrative data

- Data Security (cont.)

- Restricted availability to data down to the field level
- Multiple authorizations to request access to data
- Encrypted data and SSL security
- Auditing at the field level on all PII (personal identifiable information)
- Maintain all software with the latest updates and patches available
- Regular meetings with vendors to keep current on emerging issues and technologies

- Compliance

- Compliance with all state and federal statutes

- Family Educational Rights and Privacy Act (FERPA)
 - Children's Internet Protection Act (CIPA)
 - Health Insurance Portability and Accountability Act (HIPPA)
 - Student Data Privacy Act (KSA Senate Bill 367)
 - Olathe Public School's Board of Education Policy IDAE

- Security Analyst on staff to oversee, monitor, test, report and make recommendations of all aspects of network and data security

- Personnel – the most important aspect of security
 - All new staff attend orientation which includes ethics and security training
 - Annual ethics and security training for all returning staff
 - Monthly internal security meetings with Security Analyst
 - Quarterly meetings with building staff responsible for student data
 - Continuous monitoring of user accounts
 - Bi-Annual audit review of user access

Olathe Public Schools has a strong commitment to safety and security in all areas across our district, not the least of which is the security of our network systems and data.

The Technology Division's philosophy is to Manage Things and Lead People to provide a safe, secure and technology enriched education for our students.