Jefferson County Public Schools

Information Security

August 2025 Update

How does JCPS IT Identify, Mitigate, and Manage Technology Risks?

Risk Management

Continuous Improvement

Conformance with the KDE Data Security &
Breach Notification Requirements

Balance digital safety, privacy, and security while supporting instruction and daily operations.

Cybersecurity Threat Landscape

Between July 2023 and December 2024
- **82% of reporting K-12 school districts experienced cyber threat impacts** (5000 K-12 institutions studied)
- **14,000 security events**
- **9,300 confirmed security incidents** *(2025 CIS MS-ISAC Cybersecurity Briefing)*

- Top threats: **Ransomware attacks, Malvertisement, Phishing, Data breaches, Denial-of-Service** *(2025 CIS MS-ISAC K-12 Cybersecurity Briefing*)

Alarming trends:
- Increased attack on the human element, targeting critical academic periods, exploiting staff and students' reliance on digital tools

Map of Cyber Incidents against K-12 Districts from 2012 - 2023
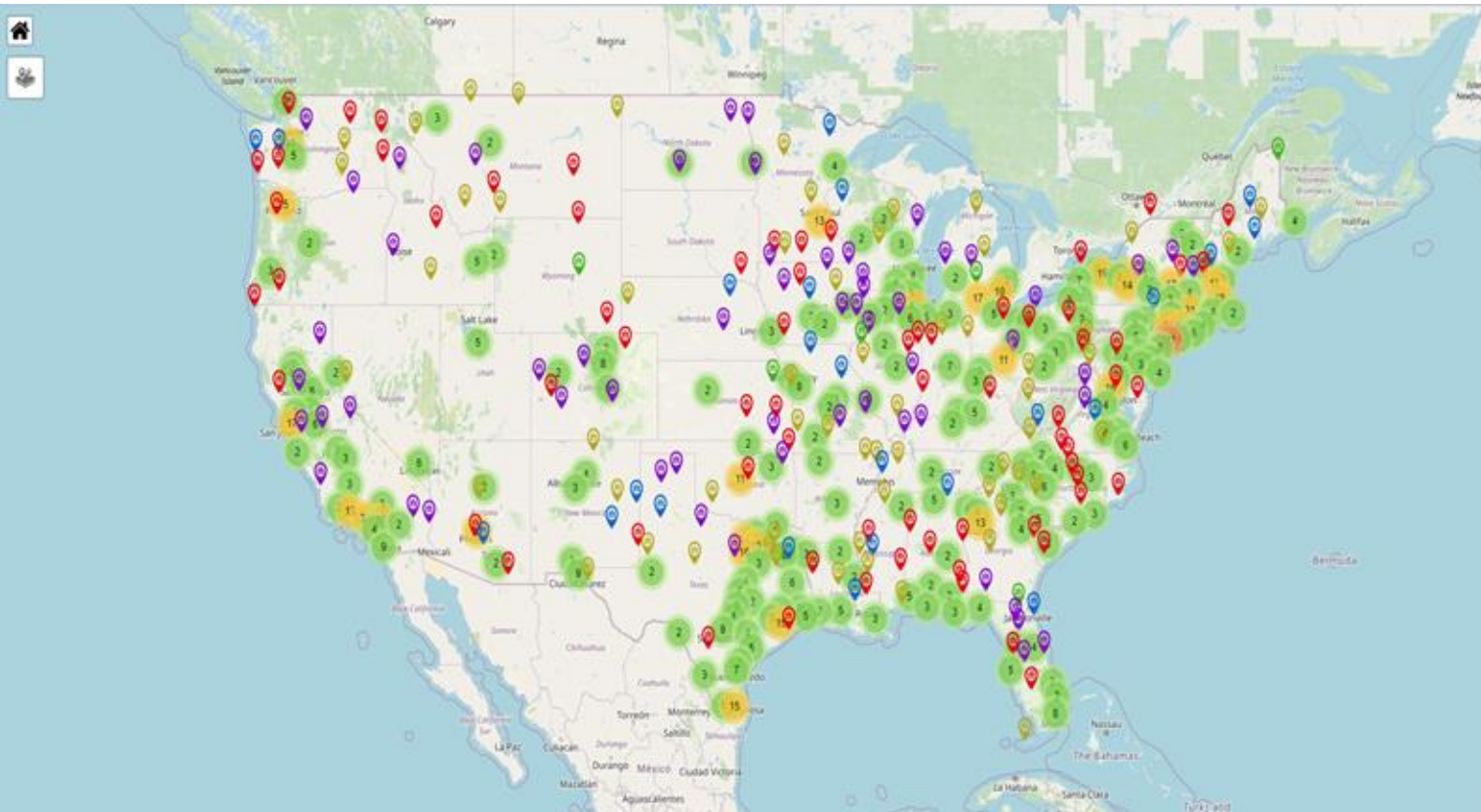
1,619 Incidents tracked by K12SIX

IT Risk Management

- Policy and Procedures aligned with the National Institute of Standards and Technology Cybersecurity Framework

- Digital Resource Review (DRR)

- Risk Register

- Partnering with CISA to improve the district's security posture

IT Risk Management
Continuous Improvement

Highlights

- Awarded funding through FCC Cybersecurity Pilot
- Improved Organizational Structure
- Endpoint Management
- Identity and Access Management
- Logical and Physical Controls
- Augment Information Security Posture
- Increased Focus on the Human Element
- Increased Focus on the NIST Domains
- Independent Assessment