

DATA SECURITY & PRIVACY

ANNUAL BOARD OF EDUCATION PRESENTATION



PRESENTATION PURPOSE

Awareness, Compliance, and Implementation

1. Basic awareness of data security and privacy best practices.
2. Mandatory notification to the Board that the District has reviewed and implemented KDE best practices.

FEDERAL AND STATE FRAMEWORK



FERPA

The Family Rights and Privacy Act (1974) protects the privacy of student education records.



COPPA

Children's Online Privacy Protection Act (1998) regulates the collection of personal data from children under 13.



KRS STATUTES

Kentucky-specific laws (HB 5 & HB 232) that define personal info and mandate security protocols.

DEFINING SENSITIVE DATA

PERSONAL INFORMATION (HB 5)

Unlike FERPA's general PII, HB 5 specifically targets elements that lead to identity theft:

- Social Security & Taxpayer ID Numbers
- Driver's License or Unique Student ID Numbers
- Biometric prints and digital images
- Financial account numbers combined with access PINs



THE "WHY" OF DATA BREACHES



HUMAN ERROR

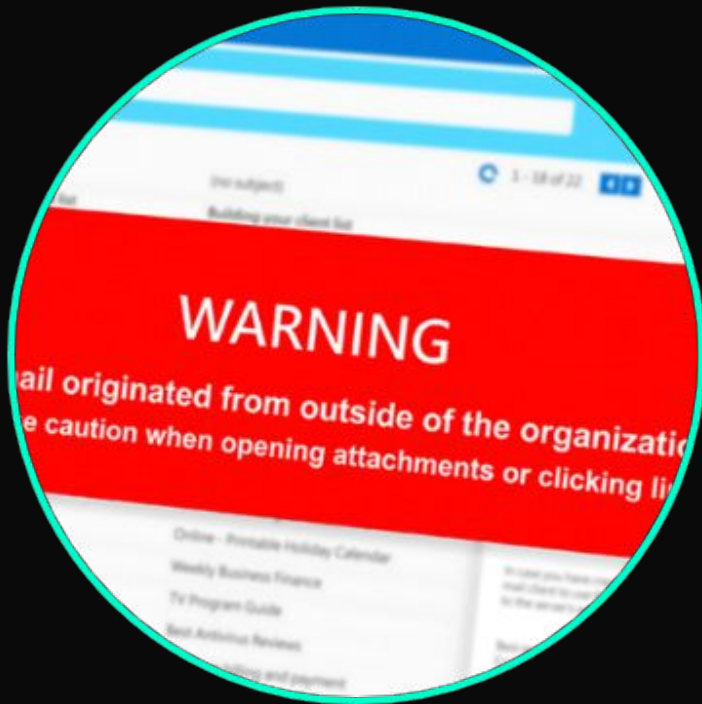
Accidental sharing via email/web, weak passwords, and loss laptops or USB drives remains the leading cause.



TECHNICAL RISKS

Phishing schemes (top threat in KY), application vulnerabilities, unpatched software, and targeted malware attacks.

CRITICAL THREAT FOCUS

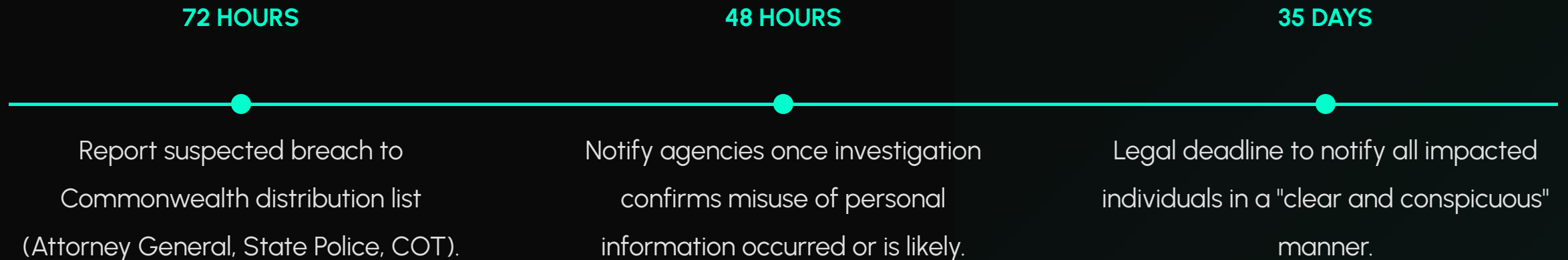


#1 THREAT: PHISHING

Phishing remains the most common data breach cause in Kentucky K-12 districts. Victims are tricked into voluntarily giving away credentials or clicking malicious links.

Our Defense: Enhancing data and network security through mandatory annual staff privacy training, strict password governance, and automated access controls to ensure permissions are granted and revoked appropriately."

MANDATORY NOTIFICATION TIMELINE



CURRENT DEFENSIVE MEASURES

- > **Network Integrity:** Firewalls, Web filtration, and DDoS mitigation.
- > **Device Security:** Anti-virus/malware, encryption, and system patch management.
- > **Access Control:** VPN support and Active Directory/Group Policy implementation.
- > **Vulnerability Audits:** Periodic scanning to identify and remediate weaknesses.
- > **Account Management:** Immediate removal of user accounts for staff no longer employed.
- > **Secure Transfers:** Encrypted file transfer protocols for sensitive document sharing.
- > **State Standards:** Adherence to enterprise security policies (CIO-090, 091, 092).

CLOUD VENDOR COMPLIANCE

Requirement (KRS 365.734)	Standard for Cloud Providers	Examples
Data Processing	Only for improving services; no advertising.	Infinite Campus
Sale of Data	Strictly prohibited; data remains student property	Google / MS
Certification	Must certify in writing compliance with KY law	Pearson / WIDA
Security Controls	Maintain student privacy pledges and safeguards.	Clever

**All vendors must comply with the Student Privacy Pledge.*

QUESTIONS?

Protecting Student Privacy is a Shared Responsibility.