Estill County Schools – Annual Data Security and Privacy Overview for the Board of Education
Prepared by: Jeremy Simpson
Presented to: Estill County Board of Education

Purpose

This annual overview is designed to inform the Estill County Board of Education about the state of data privacy and cybersecurity within the district. It aligns with the requirements outlined in **702 KAR 1:170**, Section 3, and incorporates best practices from the Kentucky Department of Education's (KDE) cybersecurity guidance. The purpose is to ensure transparency, enhance board understanding, and support informed decision-making around technology risk, investment, and strategy.

Key References

- **702 KAR 1:170** – Annual Reporting Requirements:
  https://apps.legislature.ky.gov/law/kar/702/001/170.pdf

- **KDE Best Practices for Data Security**:
  https://education.ky.gov/districts/tech/Pages/Best-Practice.aspx

- **HB5 (KRS 61.931–61.934)** – Data Breach Notification Requirements:
  KRS 61.931
  KRS 61.932
  KRS 61.933
  KRS 61.934

Recommended Topics for Annual Board Review

While each district may tailor its presentation, the following topics are strongly recommended for inclusion in the annual board update:

1. Understanding Legal Obligations

- Overview of Kentucky data privacy laws (HB5).
- Definition of a data breach and notification obligations.
- Familiarity with roles of legal counsel in breach response.

2. District Data Landscape

- Types of data managed (student, staff, vendor, operational).
- Critical systems used (e.g., Infinite Campus, MUNIS, food service, library, transportation).
- Data storage practices and backup contingencies (on-premise/cloud, recovery capabilities).

3. Security Posture and Risk Assessment

- Known district-specific risks (e.g., phishing attempts, ransomware incidents, weak passwords).
- Summary of the current security strategy:
    - Password management improvements
    - Awareness campaigns and staff training
    - Email safety measures (DMARC, DKIM, Safe Links, Safe Attachments)
    - Device security (encryption, local admin rights policies)
    - Incident response planning and drills

4. Initiatives Underway

- Planned improvements (e.g., Multi-Factor Authentication, MS A3/A5 licensing, stale account cleanup).
- Security tools implementation (endpoint protection, mail filtering, access control).
- Resource limitations or barriers (e.g., staffing, funding, resistance to change).

5. Ongoing Challenges

- Gaps in security capabilities (e.g., inability to encrypt sensitive emails).
- Staff shortages to respond to incidents like malware outbreaks.
- Persistent operational habits (e.g., password sharing, unlocked access points).

6. Successes and Progress (“Wins”)

- Awareness training sessions completed.
- Security features implemented or upgraded.
- Reduction in incidents or improved response times.
- External audits or penetration tests completed.

Sensitive Information Consideration

While transparency with the Board is vital, public meetings should avoid disclosing specifics about the district’s current security technologies or vulnerabilities. A private session or follow-up with district leadership is recommended for detailed discussions. This protects the district from malicious actors who may exploit disclosed weaknesses.

Final Notes

- This report should be adapted annually to reflect changes in systems, threats, and resources.

- Districts are encouraged to collaborate and share non-sensitive versions of their reports for benchmarking.

- The goal is to create a consistent and informed conversation between district technology leaders and the Board, with a focus on continuous improvement and legal compliance.

Prepared by:
Jeremy Simpson
DTC/CIO
Estill County Schools
jeremy.simpson@estill.kyschools.us