Comprehensive Data Security and Compliance Report

Introduction

This report outlines the measures taken by our school district to ensure compliance with Kentucky state law 702 KAR 1:170 (3) regarding the protection of personal information and the implementation of robust data security practices. It also details additional steps undertaken to enhance the overall security posture of our email and network systems for staff and administrators.

Compliance with Kentucky State Law 702 KAR 1:170 (3)

Kentucky state law 702 KAR 1:170 (3) mandates that each public school district annually review and consider the most recent best practice guidance for personal information and reasonable security. This includes, but is not limited to, the Data Security and Breach Notification Best Practice Guide. In adherence to this requirement, our district has conducted a thorough review of this guidance.

We confirm that the data security policies currently in place have been meticulously reviewed for full compliance with the Kentucky Department of Education (KDE) Data Security and Breach Notification Best Practice Guide. This review ensures that our policies align with the recommended standards for safeguarding sensitive personal information and establishing effective protocols for data breach notification.

As required by the statute, this acknowledgment will be presented to our local board during a public meeting prior to August 31 of this year, confirming that the district has reviewed this guidance and implemented the best practices.

Enhanced Email and Network Security Measures

Beyond the mandated compliance, our district has proactively taken significant steps to bolster the security of our email and network infrastructure. These enhancements are designed to provide a more resilient defense against unauthorized access and cyber threats, thereby protecting the data of our staff and administrators.

Key security measures implemented include:

- **Multi-Factor Authentication (MFA):** We have successfully implemented Multi-Factor Authentication for access to all our critical systems. This adds an essential layer of security by requiring users to provide two or more verification factors to gain access, significantly reducing the risk of unauthorized access even if a password is compromised.

- **Geographic Access Restriction:** To mitigate risks associated with international cyber threats, we have implemented a policy to deny access to our systems for any request originating from outside the United States of America. This geographical restriction acts as a crucial barrier against a common vector for cyberattacks.
- **Continuous Threat Monitoring:** We utilize resources from the Cybersecurity and Infrastructure Security Agency (CISA) on a weekly basis to monitor for emerging threats and vulnerabilities, ensuring our security posture remains current and adaptive.

Conclusion

Our district remains committed to upholding the highest standards of data security and privacy. By adhering to Kentucky state law 702 KAR 1:170 (3) and proactively implementing advanced security measures such as Multi-Factor Authentication, geographic access restrictions, and continuous threat monitoring, we are dedicated to protecting the personal information of our students, staff, and administrators, and ensuring the integrity of our digital infrastructure. We will continue to monitor evolving best practices and technologies to maintain a robust and adaptive security framework.