2023-2024 Data Security Update

702 KAR 1:170

Summary

702 KAR 1:170 requires that the district acknowledge to its local board prior to August 31 of each year that it has reviewed the guidance of the KAR and implemented best practices. This presentation on data security and privacy completes the requirement.

Objective

Provide basic awareness of of data security and privacy best practices

Notification to the Dawson Springs Board of Education that the district has reviewed and is working to implement best practices.

KDE Best Practice Guide - Notification

Immediately

Procedures and practices to safeguard against security breaches must be implemented by any entity that maintains or possesses personal information in accordance with applicable KRS and federal laws.

For any contracts involving personal information that are entered into or amended after January 1st, 2015, specific language requiring protection of the data must be included.

KDE Best Practice Guide - Notification

Within 72 Hours of Suspected or Confirmed Breach

1. Send notification, via the FAC-001 form, to the Department via email to the **KDEDataBreachNotification@Education.ky.gov** and to the following agencies as required by KRS 61.933:

- Attorney General's Office
- Auditor of Public Accounts
- Finance and Administration Cabinet
- Kentucky State Police e. Kentucky Department of Library and Archives f. Commonwealth Office of Technology

Upon notification to the Department at the email address the **KDEDataBreachNotification@Education.ky.gov**, the Department shall provide the school district the most current contact information for the notification to the other agencies required by KRS 61.933. If there is an ongoing investigation involving law enforcement which prevents information being disclosed to the Department, use the FAC-002 form to provide the notification required by KRS 61.933.

2. Begin conducting a "reasonable and prompt" investigation to determine "whether the security breach has resulted in or is likely to result in the misuse of personal information."

KDE Best Practice Guide - Notification

Within 48 Hours of Completion of the Investigation

Notify the above staff contacts if the investigation finds that the misuse of personal information has occurred or is likely to occur. The length of the investigation is not set, and will vary with each instance.

KDE Best Practice Guide - Notification

Within 35 Days of Suspected or Confirmed Breach

Notify all individuals impacted by the breach in a manner required by KRS 61.931, et seq. including information required by the Act. If breach impacts more than 1,000 individuals, nationwide consumer reporting agencies must also be notified. KDE recommends notifying affected individuals as soon as possible and not waiting until the 35th day.

If the investigation determines that misuse of personal information has not occurred or is not likely to occur, notification of the impacted individuals is not required, but records of the decision and evidence must be kept. Notification of the agency contacts, above, is still required noting that misuse of personal information has NOT occurred.

KDE Best Practice Guide - Management

Protection and Prevention

Organizations must implement an effective incident response program that includes pre-incident preparation; detection and analysis; containment; mitigation and recovery; and post-incident activities. Proper preparation (e.g. staff education, a healthy data diet) and awareness of legal and ethical issues are crucial.

An organization should protect the confidentiality of personal information whether it pertains to customers, employees, parents or students. For both paper and electronic records, these components include physical, technical and administrative safeguards.

KDE Best Practice Guide - Management

Do the Basics

Strong Passwords/Passphrases and change them often

Password/PIN protect all devices, including laptops, tablets, and smartphones.

When Staff Depart

- Change security entry codes/locks for buildings/rooms containing sensitive information.
- Removing old (stale) user accounts from all systems.

Ongoing employee training and communications

KDE Best Practice Guide - Management

Keep Accurate and Updated Data Inventories

Inventory all of your records systems (electronic and paper storage media) to identify those containing any type of personal information. This will help you decide what level of protection is necessary for each system, and what priority it has in your educational process.

KDE Best Practice Guide - Management

Healthy Data Diet

Collect the minimum amount of personal information necessary to accomplish your educational purposes and retain it for the minimum amount of time necessary.

KDE Best Practice Guide - Management

Classify the Data

Classify information in each paper and electronic records system according to sensitivity and the level of risk if that information was accidentally or intentionally accessed by anyone without a need to know.

A simple rule of thumb that can be used to quickly identify the data that has the highest levels of sensitivity and confidentiality in an organization would be to reflect on whether the data could be posted on a public website or viewed by anyone making an open records request

KDE Best Practice Guide - Management

Intruder Detection

Use appropriate physical and technological safeguards, such as video surveillance or alarms on buildings or rooms, to protect personal information, particularly higher-risk information, in paper as well as electronic records.

KDE Best Practice Guide - Management

Vendor Management

Require service providers and educational partners who handle personal information on behalf of your organization to follow your security policies and procedures as well as state and federal laws (such as HBs 5, 232 and COPPA).

KDE Best Practice Guide - Management

Encryption

Wherever it makes sense, such as devices used to host or access high-risk information, use data encryption in combination with host protection and access control. Pay particular attention to protecting higher-risk personal information on laptops and other portable computers and mobile storage devices (e.g. smartphones, CDs, thumb drives).

KDE Best Practice Guide - Management

Records Retention

Dispose of records and equipment containing personal information in a secure manner

Document Your Security

Have a security plan and review it at least annually or whenever there is a material change in educational practices, delivery mechanism, where the data is stored and how it accessed that may reasonably implicate the security of sensitive personal information.

Data Systems

MUNIS

Infinite Campus

MOSAIC

Google

Microsoft 365

Biggest Risks to K-12 Education

Phishing Scams

Poor Password Hygiene

Malware

Local Admin Permissions

Human Error

Efforts to Increase Security

Enhanced Default Password Policy

Single Sign On for Infinite Campus access

Account Automation for student accounts

Email Encryption

Email Attachment Scanning

Conditional Access Policies for Staff and Students

Company Branding on all Microsoft 365 sign in pages

P.I.I blocking alerts for Microsoft 365 services

Local Admin Accounts Removed

Lock Screen Timers

Staff/Student Identification

Efforts to Increase Security Cont.

Anti-Virus/Malware/Spam Protection

Ransomware Policy through KDE

Locked Data Centers

Locked Record Management Areas

System Patch Management

Content Filtration

Managed Firewall

External Email Alert Banner

Regular Network Updates/Maintenance

Restrict Google Access outside of our domain

Staff MFA Implementation

Infinite Campus Rights Delegations

Staff Awareness Training

Implemented

Password Security Training (SafeSchools)
Due 9/30

Data Awareness Handout/Presentation (Tech Department)
Due 9/1

Data Awareness Handout Checkpoint (Tech Department)
Due 3/30

Reminder Emails (Tech Department)
As Needed

Will Implement

Staff MFA Setup 8/30

Browser Security Basics (SafeSchools) 9/30

Email and Messaging Safety (SafeSchools) 9/30

Visitor Management Solution 10/31

Relevant Links

KDE Data Privacy and Security Homepage

KDE Data Breach Best Practice Guidelines

KDE Data Breach Awareness Guide