Data Security and Breach Notification Best Practice Guide

Kentucky Department of Education (KDE)

V2.2 September 2015

Kentucky Department of Education
500 Mero Street
Frankfort, KY 40601
(502) 564-2020

Special Note:

This guide is a living document and subject to change. Districts will be alerted to major changes, which could occur at any time. Otherwise, updates to this document will be available each August.

Version Control

Version	Date	Author	Change Description
2.0	4/22/2015	R. Hackworth	Adapted from 2006 HB 341 Data Security Study
2.1	4/24/2015	R. Hackworth	Added “version control.” Added “Resources” section with webcast archive & COT document links at end of document. Changed links for HBs 5 and 232 docs to highlighted versions used during noted webcast.
2.2	7/20/2015	R. Hackworth	Added data breach notification distribution list

Overview

In 2006, the Kentucky General Assembly passed House Bill 341, which mandated the Kentucky Department of Education (KDE) to conduct a study of the requirements for data security and a notification process when a data breach occurs.

The intent of the study requested by the legislature was to provide some general guidelines and recommendations to KDE and school districts related to some basic measures that can be considered to protect and prevent the access to restricted personal information by any person that does not have the proper access rights, authority or the "need to know" (a.k.a., an unauthorized person) and to provide some considerations and protocols in regards to notifying any affected individual should this type of information be made available in paper or electronic form to any unauthorized person.

Since that legislation, the threat and occurrence of data breaches has only increased. The House Bill 341 data security study has remained an effective cornerstone of guidance, and new legislation has added clarity, definition, and direction. But, as technology and how we use it in the schools has changed, so must that original guidance. This document, while incorporating the still-relevant guidance of the HB 341 study, will supersede it.

One thing that has not changed, however, is KDE's role. Since the Kentucky Educational Technology System (KETS) began in the early 1990s, districts have possessed the authority and responsibility to ensure their own security, whether it be part of the network, data system or even paper documents on a desk. KIDS does not have the staff or desire to begin inspecting, approving, disapproving, or monitoring each district's reasons or detailed actions in implementing or not implementing suggested best practices. However KIDS staff will be a resource for any questions or suggestions for additions/edits a district has throughout the years in regards to the reg and the best practice guideline. Any district wanting anything beyond that (e.g., an annual inspection, confirmation, thumbs up of their data security, a professional opinion on which data security recommendations should or shouldn't be implemented within their district, etc) will be pointed to resources outside of KDE (see "Remediation, below) that can best help them with the types of task/services.

On January 1, 2015, a new state law, the Personal Information Security and Breach Investigation Procedures and Practices Act (KRS 61.931, et seq.) went into effect. This legislation is more commonly known as "House Bill 5." This Act concerns the protection of personal information and applies to every state agency, including KDE, every public school district, and every vendor with which we have contracts. While this document incorporates best practice that we are all encouraged to follow, it also incorporates the "have to" actions from KRS 61.931, et seq. (HB 5).

In addition to the legal requirements, this document makes recommendations based on research and experience (best practice). However, there is no guarantee that implementing all of the recommendations will remove 100% of the risk of a data breach. Each district is encouraged to implement the recommendations that it believes are the most helpful given its perception of risk and fiscal capabilities.

This next section provides a summary of the requirements, prior to and following a suspected or confirmed data breach, from KRS 61.931, et seq. (HB 5). The remaining sections either provide more detail for these requirements or provide recommendations.

Data Breach Act "Have to" Section

Please be advised that this is a summary. A thorough understanding of KRS 61.931, et seq. (HB 5), along with its included definitions, will be very helpful and is recommended.

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.

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:

    a. Attorney General's Office
    b. Auditor of Public Accounts
    c. Finance and Administration Cabinet
    d. 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."

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.

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.

Data at Risk

Unlike the private sector or most other parts of government, a very high percentage of the data elements collected and used in P-12 schools are not considered confidential and are usually made directly accessible to any public citizen either instantly through a variety of electronic means (e.g., Web sites at schools, district offices, the Kentucky Department of Education and the U.S. Education Department) or very quickly in response to open records requests that must be provided in paper or e-mail form. Also, most of the data collected at the state and federal level are in summative form and therefore do not contain individually identifiable or confidential data.

This means that access to the majority of the truly private P-12 data is controlled by district staff, who control the permissions to these areas, systems and services. Most reside physically (e.g., on paper within cabinets, on electronic files inside a fileserver or workstation) within the district though as cloud services increase in popularity, more and more sensitive or confidential data exists outside of the district boundaries, though still under district control.

There is a category of P-12 data that is considered very personal and restricted and is becoming more and more sought after by identity thieves – the social security numbers of students. Even more than the SSNs of adults, the SSNs of children are valuable because children usually do not engage in behavior that might result in a credit check. This means the identity thief can use or sell these SSNs for years before ever having any attention drawn to them.

Most of the time, if there is an exposure of this type of restricted personal data, such as a student's medical records or a teacher's SSN, it happens accidentally (e.g., confidential personal data is printed to an unintended printer in a building, e-mailed to the wrong person or group or placed on an incorrect Web site). Also, the number of people who accidentally see confidential data that they should not be viewing tends to be limited to a small group; most of which disregard or destroy what they have seen because they do not realize that it is restricted personal data.

Yet, there are times where there are intentional attempts (e.g., a laptop or cabinet drawer containing paper files is stolen from a school, someone is just curious about a fellow employee's personal information) to access restricted personal information by unauthorized people who do not have a true need to know.

Whether the exposure happens accidentally or intentionally, the same prevention steps and notification protocols should be considered for all restricted personal data, no matter the media form (i.e. paper or electronic) that that data is stored on. In fact, most organizations already have well-established procedures for confidential personal data that is on paper form, which also can be considered for the same type of restricted data that is available and stored in electronic form.

The bottom line is that pre-emptive measures to protect and prevent the access by unauthorized people should be taken by each P-12 organization that controls and manages restricted personal information. However, if an individual's restricted personal information possibly has been seen by an unauthorized person, no matter how small or large the level of knowledgeable exposure, there is an obligation to let the affected individual know as quickly as possible that restricted personal data may have been compromised and disclosed to unauthorized people. If possible, that affected person should be informed what specific restricted data has been exposed, how long it has been exposed, who it has been exposed to and how the exposure occurred. This must be done no matter how embarrassing this announcement may be to the organization that is responsible for that

restricted data becoming accidentally exposed or a victim of its data system being successfully accessed through criminal activity.

The Three Major Areas of Consideration of Personal Data Security Management

This study was originally conducted by Kentucky Department of Education with research derived from information received from Gartner, NOREX and various state departments around the nation. Gartner provides independent research and analysis to private and public organizations over a wide range of technology subjects. Norex is a consortium of public and private companies that share their policies, lessons learned and processes with the other association members to consider for use in their organizations. Finally, a large number of states already have established legislation and policies that we can learn from without trying to reinvent the wheel. Therefore, we considered and consolidated information gathered from all these sources into a concise report that focuses on three major areas:

- Protection and Prevention
- Preparation for Notification
- Notification

1. 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.

The level of acceptable risk should be articulated, and security procedures should be balanced with available funding for information and data security, access and safeguards. In the event that more secure measures are needed, these measures should be identified for implementation and allocation of resources.

The cornerstone of improving data security is basic awareness among all staff. To promote awareness of data security best practices, the Kentucky Department of Education's Data Governance team has produced a series of three short videos focused on protecting personal information. While everyone is welcome to view and use these videos, please keep in mind they were developed specifically for KDE use and may not perfectly match every district's needs.

1. What is PII?
2. Data Access and Sharing
3. Was that a Data Breach?

Additional information about data privacy and security from KDE, the U.S. Education Department, PTAC, and others can be found on the KDE website here.

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. Among such safeguards are the following recommended practices:

- **Do the Basics** – Keep and promote awareness of basic, but extremely important, security and privacy policies related to
    - using strong passwords or passphrases and changing them often,
    - keeping a password, PIN or passcode on all devices, including laptops, tablets and smartphones,
    - whenever staff depart:
        - changing security entry codes/locks for buildings/rooms containing sensitive information
        - removing old or unused user accounts from all systems
    - ongoing employee training and communications.

  This should help reduce the number of incidences or magnitude of exposure of very sensitive data, while at the same time increasing the speed of proper notification and protocol should this exposure occur.
- **Keep Accurate and Updated Data Inventories** - Inventory all of your records systems (e.g., 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 processes.
- **Have a Healthy Data Diet** - Collect the minimum amount of personal information necessary to accomplish your educational purposes, and retain it for the minimum time necessary.
- **Classify 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.
- **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.
- **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 has developed the following verbiage, which, if used by any district, must be customized, for inclusion in contracts:
    - KDE RFP Attachment - Data Security and Breach Protocols
    - KDE RFP Attachment - FERPA and Affidavit of Non-Disclosure

- **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).

- **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.

2. Preparation for Notification of Affected Individuals

- **Leading the Charge** - Designate an individual, such as the CIO, as responsible for coordinating your internal investigation and notification procedures for the paper and electronic restricted personal data for which you are responsible.
- **Data Breach Policy -** Outline investigation and notification procedures to be followed if the school district determines or is notified of a security breach of personal information, including notice to the individual whose personal information was breached or to the parents of an individual under eighteen (18) years of age whose personal information was breached, documentation of the event, and a process for the parents or individual to request a debriefing session regarding the breach.
    - Consider suggestions from law enforcement with expertise in investigating crimes that use technology (e.g., hackers breaking into fileservers) and nontechnology (e.g., burglars breaking into buildings) means for intentionally accessing unauthorized restricted personal information for inclusion in your incident response plan.
    - Consider suggestions from your legal staff during planning. They have the greatest knowledge and expertise on what data does and does not meet the requirements of the open records law. This means they can be very valuable in helping you identify the most restricted personal data in your organization. They also can help you craft the wording for your written or verbal notifications that must be provided when an exposure occurs. They can point you to the most appropriate law enforcement official to contact should criminal activity be the reason the data became exposed or if the exposed data is possibly being used for criminal purposes (e.g., identity theft, fraud).
    - Adopt written procedures, in accordance with data breach legislation, for notification of individuals whose unencrypted notice-triggering personal information have been, or are reasonably believed to have been, acquired by an unauthorized person. Notification can take many forms that include a face-to-face meeting, a phone call, posting on a Web site or sending a paper notice to each affected person's home. The number of people that need to be contacted will usually influence the form of notification that is chosen and how quickly each person can be reasonably notified
- **Training -** Regularly train employees, including all new, temporary and contract employees, in their roles and responsibilities in your data breach policy/incident response plan. It is also important to make sure everyone is familiar with key terms such as "confidential," "PII," and what, exactly, defines a breach.
- **Remediation -** In addition to the notification of state agencies, each district, just like KDE, is expected to be able to remediate the issue which allowed the breach to occur. Plan for and use measures to contain, control and correct any security incident that may involve higher-risk personal information. Multiple options are available.

- Many IT auditing firms can offer forensic/recovery/notification services in addition to pre-incident vulnerability auditing for potential weaknesses. Districts are encouraged to inquire with their existing auditors for these services.
- Check the Best Practice Guidelines page on the KDE website for the current state contract holder for security services, including vulnerability assessment and forensic investigations.
- Also check with other state contract holders, such as for anti-virus products, which may provide additional security services and also be helpful.
- The Commonwealth Office of Technology also offers various security services available to all state agencies and public school districts.
- The United States Computer Emergency Readiness Team (US-CERT) offers a free or facilitated Cyber Resilience Review "to evaluate an organization's operational resilience and cybersecurity practices."

- **Whom to Call** - Identify appropriate law enforcement contacts to notify on security incidents that may involve illegal activities. Keep important numbers handy.
- **Documentation** – As soon as a potential breach occurs, it is important to document the issues found and response actions taken on an incident.

Reflect and Review - Review your incident response plan at least annually or whenever there is a significant change in your educational practices or how the data can be accessed electronically or in paper form. It is also important, after a security incident, to reflect on what worked well, and perhaps not so well, and then make changes to your process.

3. Notification

As of January 1st, 2015, Kentucky began to require notification of suspected or confirmed data breaches. With the passage of KRS 61.931, ET SEQ. (HB 5), Kentucky public agencies and public schools are required to notify both the individual victims of a breach and various state officials.

House Bill 5 addresses the safety and security of personal information held by public agencies and requires public agencies and nonaffiliated third parties to implement, maintain, and update security procedures and practices, including taking any appropriate corrective action to safeguard against security breaches.

- House Bill 5 document with Highlighting

House Bill 232 has two sections. Section 1 requires consumer notification when a private party data breach reveals personally identifiable information. Section 2 requires cloud computing service providers contracting with educational institutions to maintain security of student data.

- House Bill 232 document with Highlighting

In addition to this legislation, districts are encouraged to review the following links, which provide helpful information regarding contractual arrangements with cloud service providers:

- Gartner insights: 3 important questions to ask your potential cloud provider http://intersog.com/blog/gartner-insights-three-important-questions-to-ask-your-potential-cloud-provider/

- Infoworld – Gartner: Seven cloud-computing security risks http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0
- Gartner: Cloud Exit Strategies http://blogs.gartner.com/kyle-hilgendorf/2013/09/18/cloud-exit-strategies-you-do-need-them/

Required Data Breach Notification Forms

As noted in House Bill 5, the following forms, developed by the Commonwealth Office of Technology, are to be used to notify all required agencies in the event of a breach or a suspected breach of data.

- Data Breach Notification Form FAC-001
- Delay of Notification Form FAC-002

The purpose of notifying individuals of such incidents is to enable them to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm. To ensure giving timely and helpful notice to affected individuals, the following practices are required by Kentucky's data breach legislation:

Contents of Notification

1. To the extent possible, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired;

2. Contact information for the notifying agency, including the address, telephone number, and toll-free number if a toll-free number is maintained;

3. A description of the general acts of the agency, excluding disclosure of defenses used for the protection of information, to protect the personal information from further security breach; and

4. The toll-free numbers, addresses, and Web site addresses, along with a statement that the individual can obtain information from the following sources about steps the individual may take to avoid identity theft, for:
    - The major consumer credit reporting agencies;
    - The Federal Trade Commission; and
    - The Office of the Kentucky Attorney General.

Timing of Notification

- According to the data breach legislation passed in 2014 and that went into effect January 1st, 2015, each agency and public school has a total of 35 days from the time of their formal notification of agency contacts to "notify all individuals impacted by the security breach." Details about the type of notification, which can impact the cost, can be found in the legislation.

Contact Law Enforcement

- If your assessment leads you to reasonably believe that an unauthorized person through criminal activity versus by accident acquired restricted personal information, then a notification to law enforcement, such that would begin an investigation, should occur as well. This is over and above the notification required by KRS 61.931, ET SEQ. (HB 5).

Cost Considerations When Implementing Personal Data Security

Please note that none of the other states and private organizations identify the total cost to fully implement all three major areas mentioned above. But if cost was mentioned, it was a cap amount that had to be spent in notifying people of a potential compromise of their personal data. A cap is something that should be considered by the department and school districts.

KDE and every public school district will need to weigh the risk of a data security breach versus the cost to implement these recommendations. Some of the suggested items listed under Protection and Prevention can be very expensive to implement (e.g., encryption, intrusion detection systems), so some owners of data systems will implement these, and others will take their chances and will do the best they can with the methods they are now using. This will cause the costs to fully implement all the recommendations mentioned above to fluctuate greatly between all the different paper and electronic data systems in school districts and KDE. This makes it very difficult to estimate overall cost to implement statewide at this time. It is, however, fair to ask each organization to prepare for and implement these three major areas the best they can, while at the same time placing a cap on what must be spent toward actual notification.

Additional Resources

April 23, 2015 HB5 Kentucky K-12 Data Breach Webcast Archive
Direct link:
http://mediaportal.education.ky.gov/technology/2015/04/hb5-kentucky-k-12-data-breach-webcast/

Short link:
http://mediaportal.education.ky.gov/?p=3606

Additional Commonwealth Office of Technology Resources

COT has the following enterprise policies in place that may assist meeting requirements for KRS 61.931, et seq. (HB 5) for "Reasonable security and breach investigation procedures and practices…" Districts are encouraged to review these documents and use them as examples, but customization will be required. These documents are written for COT and agencies in the Executive Cabinet of state government. Several of the processes within, such as contacting the Commonwealth Service Desk after an incident, will not be applicable for school districts.

- CIO-090 - Information Security Incident Response Policy
  Identifies the necessity and procedures for agencies and COT to identify and notify appropriate personnel when a security incident occurs.
- CIO-091 - Enterprise Information Security Program
  Aligns the Commonwealth's Enterprise Information Security Program with the security framework of the current National Institute of Security Standards (NIST) Special Publication 800-53.
- CIO-092 - Media Protection Policy
  Ensures proper provisions are in place to protect information stored on media, both digital and non-digital, throughout the media's useful life until its sanitization or destruction.

Data Security Measures Already in Place For KDE and Public School Districts

- Anti-Virus/Malware/Spam/Spyware Protection
- Vulnerability Scanning
- System Patch Management
- Cloud/Offsite Resources
- Active Directory/Group Policy Objects
- Private IP implementation
- Distributed Denial of Service (DDOS) Mitigation
- Web Filtration
- Centrally Managed Firewalls
- Virtual Private Network Support
- Secure File Transfer
- Statewide Product Standards

KDE and district data housed physically in Frankfort are also protected by physical security

- Code Entry Systems to General Building (Logging System)
- Staffed Reception Area
- Visitor Sign In/Out
- Isolated Code Entry for Data Rooms (limited access)
- Monitor lock down systems (CYBEX)
- Power UPS Backup System
- Locked Rack Systems
- Closed Circuit Television Video Surveillance System with Video Capture at 15 Fountain Place and 14th floor, Capital Plaza Tower.
- Entry Intrusion Alarm Systems
- Systems located at the COT data facility take advantage of 24 hour security and authorized, escorted entry only