Dear Board Members,

As you may recall, in 2014 the Kentucky General Assembly passed a bill creating Kentucky statutes KRS 61.931-61.934. These statutes provide a definition for “personal information”, and detail responsibilities for state agencies and school districts to ensure protection of data falling within the definition of “personal information” and actions to take if a breach of this information occurs. Pursuant to the authority under these statutes, the Kentucky Board of Education (KBE) promulgated 702 KAR 1:170, which requires the Kentucky Department of Education (KDE) and school districts to annually acknowledge to their respective boards, by August 31 of each year, that the department or school district has reviewed best practices that meet the needs of personal information reasonable security. This message is designed to provide assurance to the Elizabethtown Board of Education that this has occurred.

With advice from industry and Kentucky’s public school districts, the KDE developed and shared best practices for the security of data systems with all 173 districts, including Elizabethtown. Not every best practice is appropriate or even possible to implement for each data system due to functionality requirements that might be hindered by security mechanisms, expense of adding security mechanisms or retrofitting a system, or the level of sensitivity of the data. It should always be noted that, despite the amount of security features implemented and the best of intended precautions, there is never a guarantee of 100% security. There also has to be buy-in by each staff member to follow those best practices.

By default, the Elizabethtown School District employs a great number of security mechanisms such as product standards, firewalls, physical access and electronic account access controls, video surveillance, etc. to protect access, integrity and confidentiality of district data systems. It is the responsibility of each data system’s owner/manager to understand the risks associated with the systems in their charge, and to keep the appropriate, reasonable, and attainable level of security for each.

EIS is constantly reviewing and improving our security measures, and see this as an ongoing process indefinitely. If there are ever alarming or significant discoveries, EIS will make the board members aware of those, along with a risk assessment and recommendations for remediation.

Additionally, vendors of major data systems (e.g., Munis, Infinite Campus, etc.) that are used by all KY school districts and by other districts across the nation, typically have an annual IT audit conducted by an independent auditor from which a report is generated that the vendor provides to KDE and is available to be shared with every district.

To further enhance the awareness of employees, every school has been made aware of the “Data Security and Breach Notification Best Practice Guide” Also, EIS staff will annually provide each staff member with a short handout, of data security best practices titled “A Kentucky Educator’s Guide to TOP SECRET Personal Information and Data Breach Awareness”.