MEMORANDUM

TO: Randy Poe, Superintendent

Maria Brown, Chairperson

Board Members

FROM: Eric McArtor, Chief Operating Officer/Deputy Superintendent

DATE: August 1, 2016

RE: Data Security Break Review

Per 702 KAR 1:170, the district has reviewed the Data Security and Breach Notification Best Practice Guide. Best practices that have been implemented that meet the needs of personal information reasonable security in the district include but are not limited to:

* 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
* Locked Data Center
* Consistent review of processes for account creation/deletion and access to data
* Mandatory password changes (complex) for all staff annually
* Training/Communications for all district employees via email, Administrator Meetings, School Technology Coordinator Meetings