# MEMORANDUM

TO:        Matthew Turner, Superintendent
Matt McIntire, Board Chair
Board Members

FROM:     Eric McArtor, Chief Operating Officer/Deputy Superintendent

DATE:     July 30, 2020

RE:        Annual Data Security Breach Review

Per 702 KAR 1:170, the district has reviewed the Data Security and Breach Notification Best Practice Guide.  Best practices regarding data security and privacy that have been implemented include but are not limited to:

- Anti-Virus/Malware/Spam/Spyware Protection
- Vulnerability Scanning
- System Patch Management
- 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
- Forced workstation restarts
- Limit access to data based on job requirements
- 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
- Purchasing process requires cloud providers to comply with KRS 365.734 (House Bill 232 which prohibits certain uses of student data by cloud vendors)
- Multi Factor Authentication
- Surveillance cameras