Kentucky Department of
EDUCATION

Office of Education Technology

KETS Server and Storage Architectural Standard

Version 1.2 – 8/28/2024

Document Owner:	Paul Shoemaker	Date Created:	8/26/2024
Approver(s):	OET Leadership	Date Approved:	8/28/2024

Summary: This document will provide recommendations and guidance for the procurement of server and storage systems for district use. This document should be shared with district/school leaders and vendors, so they will understand these guidelines prior to selecting and offering solutions. The goal is to assist in the procurement of server and storage hardware that best serve the district and meet all necessary security and connectivity requirements before financial obligations are established or installation activity begins.

Intended Audience: The audience of this standard is District EdTech Staff, school and district leaders, and vendors/service providers. This document is to be shared within this audience to establish the need of the districts (in terms of design and general uses) while ensuring the server and storage hardware will operate successfully within the technical and security requirements of the KETS environment.

Purpose and Scope: Server and storage hardware solutions must meet certain minimum standards to ensure interoperation with other key parts of the KETS environment and be sustainable. Any data center hardware (recognized as server and storage hardware and related components for operation and usage) procured by districts must meet these standards at the procurement and throughout its usage by the district.

1. Server and storage hardware must be capable of and licensed to use current and centrally manageable modern operating systems.
2. Districts must ensure that server operating system updates and server and storage system’s firmware/driver updates are regularly and consistently installed to protect against security vulnerabilities, regardless of whether they use the KETS standard system for software updates.
3. Districts must ensure that server systems, where applicable, are capable of being protected by an anti-malware solution that is monitored and kept up to date, regardless of whether they use the KETS standard anti-malware system.
4. Districts must ensure that server systems procured by the district, that have administrative user access to the Internet, are capable of being protected by a controlled and filtered internet access solution that meets CIPA/ECF and 701 KAR 5:120 requirements, regardless of whether they use the KETS standard Internet safety solution.
5. Server systems must have the ability to be centrally managed using a system (or systems) that is capable of enforcing security requirements (such as operating system updates), configuring operating system and application updates, and monitoring and configuring anti-malware tools where applicable.

6. Solutions should consider secure remote management solutions for server and storage systems, including secure internal network access and out of band access capability to management consoles.
7. Server and storage systems should be properly scaled for their intended use. Districts should work closely with the selected vendors to tailor the solutions for proper scale of use and projected growth over the lifecycle of the proposed systems.
8. Server and storage systems should be selected with consideration of their long-term lifecycle and total cost of ownership. Server and Storage systems should have a minimum 4 to 5 year lifecycle and may have better long-term parts availability and vendor support that outweigh a higher initial purchase price.
9. Warranties should cover the lifecycle of the server and storage hardware systems. Other support arrangements or Infrastructure as a Service for server and storage systems should be selected with consideration of total cost of ownership and limited district technical staff. More expensive levels of vendor service may be worthwhile if allowing district edtech staff to focus on higher priorities.
10. Security hardening practices should be implemented that are appropriate for the usage of the system. Call the KETS service desk (866-538-7435) to schedule a security review for that server with the KETS Security Team. *ref. KETS Security Best Practices:* https://www.education.ky.gov/districts/tech/Documents/Security%20Best%20Practices.pdf