Office of Education Technology (OET)

Security Best Practices Guideline for Districts

Version 1.1 – February 24, 2017

Date Created: 1/12/2010
Date Reviewed: 2/24/2017

Summary: This document establishes a standard Security guideline for Kentucky K-12 School districts.

Purpose and Scope: These guidelines apply to all of KDE and Kentucky's 173 public school districts.

Reason for Implementing: To ensure the availability, integrity, and confidentiality of information required for normal education operations.

I. Physical Security

All District building sites with information processing areas containing equipment including but not limited to: file servers, data servers, network routers and switches, must be protected by physical controls appropriate for the size, complexity and sensitivity of the systems operated at these locations. The information and software contained within these sites should be protected from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). Physical access to information processes areas should be restricted to authorized personnel.

District leadership should ensure that all building facilities have solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

II. File, Print and Web Servers

Server Security:

1. Patch Software

    a. KDE provides security patches for Windows based systems covering security issues for a limited range of server-based products. Districts are responsible to keep software up to date and tested before applying new patches. Apple, Linux, and other operating systems should be patched as they are not part of KDE's current patch deployment system.

    b. 3rd party applications such as IIS, Java, FrontPage, .NET, etc. have their own security patches that should be applied within a reasonable time of release. District servers have been found with out of date versions of these applications due to default or pre-configured machines. Districts are responsible to keep these applications current.

2. Unnecessary Software/Services

   a. Districts should refrain from installing software not required for the intended purpose and specification of a server. The existence of MS Office or other unintended software on a web server can actually reduce the security of the box.

   b. Server security vulnerabilities are introduced with each application installed. To keep this risk to a minimum, Districts are expected to remove all unnecessary software and refrain from installation all together. Create custom installs or images for all servers when possible, avoiding the use of OEM supplied software installs.

   c. Districts should turn off unused services where possible. A web server that distributes web pages only should not have FTP or SMTP services enabled, for example. Disabling unused services reduces the attack surface and broadcasted server ports resulting in reduced security risks overall.

3. Limit Use

   a. Web servers, database servers, and file servers exist to meet a specific business need. Districts should refrain from using these servers to browse the web, run test applications, staging software installs, or adding additional services to these machines.

   b. Restrict server accounts to the access rights needed for the services and jobs performed by the server. (Ex. The District Web Administrator should not have access to a server that hosts no web content

   c. Restrict user access to only what is needed to perform the jobs assigned. Reducing access prevents configuration changes, or installation of new services and software that would decrease the security of the box.

4. Separate Public-facing Servers

   a. Servers open to the internet pose a higher risk than those available to internal users only. Those risks include attacks by bots, random scans, and other internet propagating traffic. Servers should be isolated from other servers and services by specific VLANs or separate internal DMZs. This reduces the risk of compromised servers impacting other network servers or services.

5. Periodically Check Logs

   a. Nearly all server applications or services create logs on the server. Districts are expected to routinely review the logs for patterns, issues, and unusual events. Regular review will identify required maintenance, unallocated server resources, mis-configurations, and compromises.

Desktop Security:

1. Patch Software

   a. Systems should be patched with the latest versions of software and operating system patches within a reasonable timeframe. Districts should ensure patches for Microsoft products are installed from WSUS (Windows Server Update Services).

   b. A method for timely installing 3rd party application patches should also be determined. Business required software applications such as Java, Adobe, or Flash are known to have high risk vulnerabilities not addressed within the KDE patch deployment method.

2. Anti-Virus Software

   a. All workstations should have virus scan software installed. This software must be properly configured and updated.

   b. EPO (McAfee ePolicy Orchestrator) reports should be run routinely to ensure deployment coverage and proper DAT file updates. Scheduled tasks should be configured to perform full system scans during off hours.

3. Email and Attachments

   a. Districts should educate all users of the risks associated with e-mail and promote the following good behavior:

      1) Avoid opening email attachments from un-trusted or unknown senders. Attachments are used to transfer viruses to unknowing end users. These viruses or malware can be embedded into any type of file, not just an executable.

      2) Avoid clicking active links within emails. Typically these links exist to easily access a certain part of a website or webpage. Links can lead to a spoofed page, or to a malware infected site. When presented with an active link within a webpage, navigate to the location from the vendor's direct webpage and not the active link.

      3) Never email usernames and passwords. Attackers will often lure users via email to respond to a phishing attack. These emails will vary on subjects and content, but all seem to request user specific information. Contact the District technology staff directly if this type of e-mail is received.

III. Access Control and Account Permissions

1. Formalize procedures related to the management of locked/disabled accounts on district servers

   a. Define process of disabling/removing terminated staff accounts and unnecessary generic accounts

   b. Establish a periodic review of disabled/locked accounts on all systems

2. Evaluate security groups on District servers to ensure assigned users have the appropriate access

   a. Establish a periodic review of accounts with high-level privileges to ensure they are appropriate

   b. Limit the people who have access to a system to only those who need access. Workstations in labs can cause issues with this, but stationary computers with a set amount of users can be restricted to those users who actually use or need to administrate them.

3. Limit local administrator rights to technical staff

   a. Use less restrictive account permissions when available. End users often times do not need full administrator privileges to do their day to day tasks. When end users browse or execute files, those files run at the same permission levels the user has been assigned. In the case of a system administrator, those files would then have full access to the system.

4. Strengthen password requirements as appropriate for staff/students

   a. For different user types, apply technologies such as Fine-Grained Password Policies which are outlined in the KETS Office 365 Operations Guide for AD and Messaging.

      This can be downloaded at KETS Active Directory Operations Guide.