KENAI PENINSULA BOROUGH SCHOOL DISTRICT

**Information Services**
Eric Soderquist, Director of Information Services
148 North Binkley Street Soldotna, Alaska 99669-7553
Phone (907) 714-8803 Fax (907) 262-9645

M E M O R A N D U M

TO: KPBSD Board of Education
KPBSD Administration

FROM: Eric Soderquist, Director of Information Services ES

DATE: February 6, 2017

SUBJECT: Information Regarding Digital Security Practices

With the heightened media focus on information security following the 2016 Presidential election, Information Services has received questions surrounding our digital security practices. This memo outlines the current practices in place.

Topics discussed below are general in nature. As a matter of principal, discussing specific aspects of any organizational defense-in-depth strategy is counter-productive to the established goal of securing infrastructure.

## INFRASTRUCTURE HARDENING

A primary focus over the past 10+ years has been changing internal processes to support general principals of infrastructure hardening. In this practice, the scope of infrastructure exposed to untrusted endpoints is tightly defined through deployment of devices such as firewalls.

A firewall can be characterized as any hardware or software device that can be configured with specific instructions as to the a) traffic type, b) scope, or c) endpoints identified within network traffic that are allowed to traverse or flow through the firewall.

KPBSD utilizes firewalls in three primary areas: external perimeter, internal services, and internal clients.

The external perimeter firewalls serve to define individual resources hosted within the KPBSD network that are accessible to individuals outside the bounds of the KPBSD network.

Internal server firewalls exist by default on servers deployed within the KPBSD network. These firewalls define the specific traffic allowed to reach any given server, and the configuration specifically targets those services provided by the device.

KPBSD configures internal client firewalls on each user endpoint deployed by KPBSD. These firewalls exist to define the particular traffic that can reach particular systems. Because we push

software through an enterprise system, we have a good idea of what type of network traffic is typical on our network and can configure firewalls accordingly to minimize unnecessary exposure. Client firewalls serve to mitigate risks surrounding self-propagating computer viruses.

### Network Separation

KPBSD has embraced "Bring Your Own Device" (BYOD), allowing staff and students to bring personal devices into our buildings. From an IT perspective, these devices are considered untrusted, and we take measures to prevent traffic from untrusted devices from reaching our production network. BYOD devices connecting to our network exist on a private Virtual LAN (virtual network – VLAN) that can only speak to other machines on the general internet. In this manner, a personal machine with a virus connecting to our network cannot establish network connectivity with other devices on the internal KPBSD network.

### Virus Scanning

Endpoints utilize virus scanners with real-time access scanning. Virus signatures update through an automated process to ensure no human-interaction is required to keep signatures current.

### Email Scanning

All email entering the KPBSD network is content and virus scanned. In addition, we subscribe to a number of real-time block lists designed to block known-bad emails or email infrastructure on the internet from interacting with our system.

### Enterprise Policy Configuration / Software Restriction Policies

Information Services employs a number of automated systems to manage device configuration compliance. We use these systems to ensure that configuration elements such as client firewalls are configured predictably and consistently, minimizing the risk of human error or oversight. Updates download to clients in a semi-automated fashion, ensuring that device updates occur without requiring intervention on a per-system basis.

In addition, all endpoint software installation occurs through an enterprise system, minimizing the amount of executable code, especially that which is downloaded from the internet, from being exposed to client systems. Software installations must pass through a dedicated software engineer who bundles and packages software for client distribution.

Finally, an additional layer of restriction policies exists on client endpoints that prevent executable code from running on client machines in certain locations. This allows IT control over whitelisting allowable programs, while minimizing risk due to the execution of untrusted code.

### Summary

Having a defense-in-depth strategy is critical to any IT operation. Work in this area is always ongoing, and maintaining a mutli-layered security architecture will remain at the forefront of Information Services' practice.