Policy 1170

NETWORK SECURITY POLICY

In order to prevent a breach of security to the District's network, the District has put in place the following procedure:

EQSD security is twofold.

1, BASCOM firewall server at the beginning of the network
2. Symantec Endpoint Protection on each client workstation

The BASCOM Server resides at the beginning of the network schematic so that any traffic in and out of the network needs to pass through the BASCOM server firewall. We're using a Frontera server that was installed during the summer of 2013. Inbound traffic is not allowed unless a specific rule is configured within the BASCOM firewall server. That traffic is only allowed to access the small portion of the network related to the services that they provide and the rights that we grant. This limited access is configured by the firewall rules that we set up.

Outbound traffic is controlled by Internet filter zones that are controlled by the BASCOM server. Consequently, users trying to go to malicious or unsafe sites will be blocked. Only specific administrators are granted full Internet access if necessary for valid reasons.

Symantec Endpoint Protection is enabled on all machines to prevent viruses, spyware and malicious intrusions from infecting or gaining access to individual client workstations. Network threat protection is included in Endpoint Protection.

The District will periodically review the above procedures and update as necessary.

Adopted: August 26, 2014