

MOON AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: TECHNOLOGY
SYSTEM SECURITY

ADOPTED: November 14, 2011

REVISED:

	<p style="text-align: center;">814.2. TECHNOLOGY SYSTEM SECURITY</p> <p>1. Purpose The purpose of this policy is to outline the security measures for safeguarding electronic files, documents and databases as well as maintaining the integrity of the district wide area and local area networks. This document provides the approved methods for access control measures and user authentication.</p> <p>2. Guidelines System security is protected at the network, computer, and user levels. We incorporate several layers of protection at each level. Primarily, the security protection is through the use of hardware appliances, software and passwords. Failure to implement logical access controls and protection of passwords could result in unauthorized access to technology information. At a minimum, the following security measures will be implemented.</p> <p><u>Wide Area And Local Area Networks</u></p> <p>The district network topology consists of a Local Area Network (LAN) in each of the school buildings, and a Wide Area Network (WAN) that provides connections between each building for communications to district file and application servers. Our WAN is directly connected to an Internet Service Provider (ISP). The district technology department deploys district e-mail, district web site hosting and filtered access to the Internet. The WAN incorporates a firewall, e-mail and Internet filtering, and routers to restrict access to authorized users only. The district technology director will manage and approve all access to the district network.</p> <p>The district will utilize both an “open” and “closed” network environment accessible from inside of the district. The “closed” network may only be accessed by district-owned equipment. It allows filtered access to the Internet, as well as to district resources. The “open” network, allows heavily filtered Internet access only.</p> <p>All routers, firewalls, wireless access points and other network devices will be configured and password protected.</p>
--	--

<p>Pol. 250, 815</p>	<p><u>Network Servers</u></p> <p>The district utilizes a number of file, application, and database servers. Each server has a specific purpose that varies in the degree of importance to what data is stored or accessible on that server. Therefore, the protection measures of each server may vary.</p> <p>In general, server access is controlled using Microsoft Windows Server operating system software. This software provides access control and user authentication to server information and network shares as needed. Microsoft's Active Directory with Group Policy feature provides logical control to the network, server and computer levels. The district network technician manages the access control and user authentication under the direction of the district technology director.</p> <p>All server system administrative accounts, including but not limited to database and automatic service accounts, are controlled and managed by the district technology director and subject to the password policy as described below.</p> <p><u>Network Domain Accounts</u></p> <p>Network domain user accounts control access to all district systems. Such accounts can only be created or altered (aside from password, as mentioned below) with the permission of the Personnel office. Network domain user passwords are subject to the password policy as described below.</p> <p>Access to network domain accounts and some or all network resources can be suspended due to violation of policy 815, 250, or at the discretion of the Superintendent, assistant Superintendent, or other district administrator. Network domain accounts, and all information contained therein, including but not limited to the user's home directory and email, will be deleted ninety (90) days after the termination of the relationship with the account user and the district, be that termination the result of dismissal, resignation, or end of service contract. Deletion can be forestalled with the permission of the district Superintendent.</p> <p><u>Critical Information</u></p> <p>Additional security measures are required for access to district servers and file shares that contain critical information including, but not limited to student accounting, personnel, or financial data. Access is limited by the user's employment position. The appropriate district administrator and district technology director will determine the eligibility for access to this information.</p>
----------------------	---

<p>Pol. 814.1</p>	<p><u>Remote Access</u></p> <p>The district technology director will authorize remote access to the district wide area network on an as-needed basis. Access will be controlled, monitored and reported to ensure against violations of district electronic systems usage policies. Such access may be granted to third parties for the purpose of maintenance of various systems. Should access by a third party be required, a unique network domain account will be created for each individual requiring access.</p> <p>The district will deploy monitoring tools to monitor remote access to the network. All unauthorized access will be reported to the district technology director.</p> <p>All district computers require user authentication before access is granted. Such access is a function of the network domain user accounts as mentioned in 814.1. Computer accounts local to the machine may be created by district technology personnel if required. Such accounts are subject to the same requirements as network domain user accounts.</p> <p><u>Passwords</u></p> <p>User passwords for all devices will be changed if there is a suggestion that they have been compromised; Password length will be a minimum of eight (8) characters that include alpha, numeric and special characters; a password history of (ten) 10 passwords will be kept to prevent frequent reuse of potentially compromised passwords; and users will be locked out after three (3) unsuccessful login attempts.</p> <p>Passwords for automated functions, such as databases and nightly processes, will meet the same requirements as user passwords.</p> <p>References:</p> <p>School Code – 24 P.S. Sec. 510</p> <p>Board Policy – 250, 814.1, 815</p>
-------------------	--