

Bradford Area School District

SECTION: OPERATIONS

TITLE: TECHNOLOGY
SYSTEM SECURITY

ADOPTED: SEPTEMBER 15, 2008

REVISED:

814.4 TECHNOLOGY SYSTEM SECURITY	
<p>1. Purpose</p>	<p>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 Pol. 814.1</p>	<p>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, protection of passwords as well as frequently updating 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 four school buildings that provide communications to local file and application servers and network printers; 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 email, district web site hosting and filtered access to the Internet. The WAN will incorporate a firewall, email and Internet filtering, and routers to restrict access to authorized users only. The district technology administrator will manage and approve all access to the district network.</p> <p>The district will utilize a ‘closed’ network environment accessible from inside of the district using only district-owned electronic devices. All routers, firewalls, wireless access points and other network devices will be configured and password protected. Passwords for network devices will be changed at least one each year. Password length will be a minimum of eight characters that include alpha, numeric and special characters; users will be locked out after three unsuccessful login attempts.</p>

<p>Pol. 814.2</p>	<p>The district technology administrator will authorize remote access to the district wide area network. Access will be controlled, monitored and reported in accordance with district policy 814.2 Technology Help Desk.</p> <p>The district will deploy monitoring tools to monitor access to the network. All unauthorized access will be reported to the district technology administrator.</p> <p><u>Network Servers</u></p> <p>The district utilizes a number of file, application, and database servers in each building. 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 Edition 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 administrator.</p> <p>All server system administrative accounts are controlled and managed by the district technology administrator. The system administrator passwords for each server will be changed at least once per year. Password length will be a minimum of eight characters that include alpha, numeric and special characters; users will be locked out after three unsuccessful login attempts.</p>
<p>Pol. 814.1</p>	<p>Network domain user accounts are created in accordance with district policy 814.1 Acceptable Use of Technology and Computers. Network domain user passwords will be changed at least once per year. Password length will be a minimum of eight characters that include alpha, numeric and special characters; users will be locked out after three unsuccessful login attempts.</p> <p><u>Critical Information</u></p> <p>District servers that contain critical student accounting, staff and financial information requires additional security measures. User access is limited to the user's employment position and the need-to-know. The building administrator and district technology administrator will determine the eligibility for access to this information. A separate network domain will be configured to provide an additional security layer within the network. User accounts will include the following safeguards:</p> <ol style="list-style-type: none">1. Users are required to change their passwords every 30 days,2. Password length will be a minimum of eight characters that include alpha, numeric and special characters,3. Users will be locked out after three unsuccessful login attempts.

Pol. 814.2	<p data-bbox="505 138 813 170"><u>Computer Workstations</u></p> <p data-bbox="505 212 1500 428">All district computers require user authentication before access is granted. Computer user accounts are created in accordance with district policy 814.1 Acceptable Use of Technology and Computers. Computer user passwords will be changed at least once per year. Password length will be a minimum of eight characters that include alpha, numeric and special characters; users will be locked out after three unsuccessful login attempts.</p>
------------	--