GORE BOARD OF EDUCATION POLICY

DHAC-P

PASSWORD POLICY

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Gore Public School's resources. All users, including contractors and vendors with access to Gore Public School systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Gore Public School facility, has access to the Gore Public School network, or stores any non-public Gore Public School information.

General

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.

All production system-level passwords must be part of the administered global password management database.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.

Guidelines

A. General Password Construction Guidelines

All users at Gore Public Schools should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:

o Lower case characters

o Upper case characters

o Numbers

o Punctuation "Special" characters (e.g. @#$/\&*(L +I~-=\' {}[]:";'<>/ etc)

Contain at least fifteen alphanumeric characters.

Passphrases are generally used for public/private key authentication. A public/private key system defines mathematical relationship between the public key that is known by all, and the private key, that is only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnTheIOI W as* &#!#ThisMoming"

All of the rules above that apply to passwords apply to

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the Information Security Department or its delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

Adoption Date:	***Revision Date(s): 1/28/97, 3/27/00, 8/1/00, 2/20/02***