

Pittsburgh Public Schools

Password Policy

May 25, 2005

Overview

Passwords are an important aspect of network and computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire computer network of the School District of Pittsburgh. As such, all District authorized account owners (including employees, students, parents, contractors and vendors with access to District systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. All passwords are to be treated as sensitive, confidential District information.

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 authorized account owners who have been provided an account on any computer that resides at any District building, or has access to the District network.

Definitions

Every user should be aware of how to select and use strong passwords. Users must not use weak passwords.

Strong passwords:

- contain both upper and lower case characters (e.g., a-z, A-Z)
- have digits and punctuation characters as well as letters (e.g., 0!@#%&*()_+|~=\[]:");)
- are at least eight alphanumeric characters long.
- are not words in any language, slang, dialect, jargon, etc.
- are not based on personal information, names of family, etc.

Weak passwords:

- contain less than eight characters
- are found in a dictionary (English or foreign)
- are common usage words such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.

- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word, keyboard, or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards or followed by a digit (e.g., secret1)

Responsibilities

- All system and production-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed every 90 days.
- All end user-level passwords (e.g., email, Web, windows login, SASI, Dashboard, etc.) must be changed every 90 days.
- All passwords must be a minimum of 8 characters in length and be uniquely constructed to contain both letters AND numbers.
- All user, system, and production-level passwords must conform to the guidelines and standards described below.

Application Development Standards

Application developers must ensure that their programs:

- support authentication of individual users, not groups.
- do not store passwords in clear text or in any easily reversible form.
- meet standards utilized in District applications or SSO package.

Enforcement

All user accounts provided are a privilege and the District reserves the right to revoke that privilege at anytime.

Any user who violates this policy may be subject to appropriate disciplinary action.