

SUBJECT: PASSWORD PROTECTION

Supersedes: DPS Policy 10.10 - Computer Hardware/Software and Office Equipment Use, dated July 14, 2000

Effective: February 15, 2005

Page: 1 of 2

1.0 POLICY

Through network and application accounts Detroit Public Schools (DPS) users are provided logon access to district computers, email, Internet, printing services, databases, and personal storage. Any work, whether authorized or not, is legally binding back to the individual who has been assigned the account. Account administration (logon ID and password combination) is the most cost-effective way of protecting district data. All employees (including business partners and vendors) are responsible for taking appropriate steps to select and secure their network and application passwords.

2.0 SCOPE

The scope of this policy includes all personnel who have or are responsible for an account on any system or application that resides at any DPS facility. This includes access to networks, applications, schools, or any other non-public information.

3.0 ISSUANCE OF REGULATIONS/STANDARD OPERATING PROCEDURES

The Chief Technology and Information Systems Officer has developed regulations and/or standard operating procedures to implement this policy.

4.0 FAILURE TO COMPLY

Failure to comply with this policy and/or corresponding regulations may result in a recommendation to the Chief Executive Officer for appropriate disciplinary action.

5.0 EXCEPTIONS

There are no exceptions to this policy.

6.0 AGREEMENT

I, _____ (print name) have read the Detroit Public Schools Password Protection policy, dated _____. I understand it and agree to abide by it.

Signed

Attachments: Administrative Regulation 13.05 – Password Protection

See also: None

Legal References: None

Labor Contract References: None

DETROIT PUBLIC SCHOOLS
ADMINISTRATIVE REGULATION

PASSWORD PROTECTION

This Administrative Regulation implements Detroit Public Schools Policy 13.05 – Password Protection

1.0 Password Regulations

- 1.1 All network level passwords must be changed on a quarterly basis. You will be prompted when it is time to change your network password.
- 1.2 All user level passwords (email, desktop, various applications) must be changed on a semi-annual basis. You may not be prompted to change these passwords. It is your responsibility.
- 1.3 Passwords are not to be inserted into email messages or other forms of electronic communications.
- 1.4 Do not use the same password for various access needs. Select a password for network access then select different passwords for workstation access and application level access.
- 1.5 Do not share passwords with anyone, including administrative assistants. All passwords are to be treated as confidential information. Other don'ts you must adhere to include:
 - Don't reveal a password to anyone over the phone
 - Don't reveal a password in an email message
 - Don't reveal a password to your manager
 - Don't discuss passwords in front of others
 - Don't hint at a format used to create a password (i.e. family names)
 - Don't reveal a password on questionnaires or security forms
 - Don't reveal a password to co-workers while on vacation
- 1.6 There is a rule of thumb in the security community that one should never write down a password. However, the policy we enforce is such that it is often difficult to construct a memorable password. If this is the case for your password, then you *should* write it down somewhere but make sure that it's kept in a place that is secure – in your wallet but not on your chalk board and not anywhere beside your login name!
 - Do not write down your password while you are in a public area where others could observe your writing
 - Do not identify your password as being a password

- Do not store passwords in the office area
 - Do not store passwords in a file or any computer system (including Palm Pilots or similar devices)
- 1.7 If an account or password is suspected to have been compromised, report the incident to info.protection@detroitk12.org along with changing the password if it is your account.
- 1.8 If an employee or business partner demand a password refer them to this document or have them contact the Chief Technology and Information Systems Officer.

2.0 Password Requirements

- 2.1 Minimum Length: An acceptable password must have at least seven (7) characters. Shorter passwords are easier to guess, longer passwords are harder to guess.
- 2.2 Unique Characters: An acceptable password must utilize at least three of the four different character sets. Character sets include upper and lower case letters, digits and special characters. Repeated characters can make for palindromes and reduce the search space.
- 2.3 Do not create passwords based on your name, your login name, or names of friends, acquaintances or pets
- 2.4 Do not create passwords based on personal data such as birthdays, social security number, license number etc.
- 2.5 Do not create passwords that are words in English or any other language dictionary.