



PURPOSE

The effective management of passwords is the first line of defense in the electronic security of an organization. In a school board/authority environment it is not uncommon for most employees to have multiple passwords for access to email, voice mail, computer applications, and portals. Every school board should have a password strategy in place as part of the overall security strategy.

This document is intended to be used as a guideline for developing a password procedure. It contains considerations and strategies that can be used to develop procedures for the creation and maintenance of secure passwords.

Benefits of a Password Procedure

- Appropriate access for all staff;
- Effective identity management and access auditing;
- Preservation and protection of personal information entrusted to your care;
- Protection of YOUR personal information.

Best Practices/Recommendations

The successful adoption of a password procedure depends on the ability of the organization to enforce it. Some school boards/authorities have sophisticated technologies that can provide substantial automation and support for a large number of users. Others may have limited resources and will need to develop a procedure that is manageable in a more manual fashion. It is important to realize that regardless of which category the school board/authority falls into, password procedures are still a requirement for effective security management.

When creating a password procedure, it is important to consider elements that can be enforced through software security settings and those which must be enforced through education of the users. Items such as the minimum length of a password and expiry cycle for passwords are typically set through system software. Issues that would be linked to user education include not having passwords displayed on sticky notes and not sharing passwords.

Another important consideration when developing a password procedure is password retention. Even with the best procedures in place, passwords will be shared or otherwise become known over time, weakening security, so it is necessary to change them on a regular basis. Most systems allow the system administrator to set a parameter which causes passwords to expire and requires them to be reset by the user. This parameter is typically set for anywhere from 30 days to 90 days, depending on the number of users, level of risk, and manageability of the procedure. Password expiry does add some additional workload for technical staff as users often forget their new passwords and need support to change them. It is also wise to force a password reset the first time a user logs in to any system.



Technical Considerations

- **Length of password** - Passwords should be a minimum of six characters for adequate protection but should not be too long as to be onerous for staff to remember.
- **Mixed characters** - Passwords should contain at least one of the following: upper- and lower-case letters, numbers, and special characters (@#\$!% etc). Where technology does not permit enforcement of this recommendation, it should be included in the user education.
- **Password retention** - Passwords should be reset on a regular basis and should expire after a set length of time. This can vary from 30 days to twice per year and will vary depending on the school board/authority culture and the technical support available.
- **Histories** - Password histories should be maintained and set so that users cannot use the same password twice within a defined period. The minimum history should be three passwords, but can be as high as the school board/authority chooses to set it.

User Education

For the users' protection, passwords created should be difficult to guess. The following points provide some guidance on best practices for creating a password:

- The password should not be the same as the username, even with a number or symbol added.
- Passwords should not contain personal information such as street number or name, company name, date of birth, etc.
- Passwords should never contain names of family members, pets, friends, or co-workers.
- Passwords shouldn't be a common phrase followed by a digit that is changed when the password expires.

Users should always follow these principles:

- Do not share passwords with anyone. If there is an issue that requires you to do so, remember to change the password immediately after the issue has been resolved.
- Never use the same password for work accounts as the one you have for personal use (banking, etc.).
- Do not write down passwords or include them in an email.
- Do not store passwords electronically unless they are encrypted.
- Never use the "Remember Password" feature on any systems; this option should be disabled in systems where technically feasible.



The following are some examples of both strong and weak passwords:

Password	Strength	Reason
Wam4uG	Good	Six characters, upper case and a number
sunny	Weak	Too short, too easy to hack/guess
charles1	Weak	User's first name used - too easy
22965	Weak	Same as user's personal banking PIN - poses additional risks to user
3z2tt4cy	Very Good	System-generated password which is changed every three months

Conclusion

There are many things to consider when developing a password procedure. Strict password procedures ensure greater security but require more user support and may result in a low compliance rate. Very relaxed password policies will likely result in higher compliance by users but may not provide adequate protection for school board/authority information. The key to an effective password procedure is to define a balance between the security needs of the school board/authority and its culture and to follow the guidelines defined here.

There are many valuable resources available online which can be used in conjunction with this document. The SANS (SysAdmin, Audit, Network, Security) Institute, www.sans.org, offers a password policy template that can be modified by an organization. Many school boards/authorities in Ontario have developed password policies or procedures and most are willing to share with other school boards/authorities.