

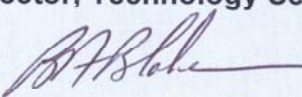
Lakehead University

Password Maintenance

Technology Services Centre

Standard Operating Procedure

Issued: 2010-08-09

Approved by:	Name: Bernie Blake
	Title: Director, Technology Services Centre
	Signature: 

Note: This SOP replaces Lakehead University original Password Policy

TABLE OF CONTENTS

1.0 General Statement.....	3
2.0 Purpose	3
3.0 Scope.....	3
4.0 Procedure.....	3
4.1 General	3
4.2 Requirements	4
4.3 Guidelines	4
5.0 Failure to comply.....	6

1.0 GENERAL STATEMENT

Username and password combinations provide privileged access to computer based information systems at Lakehead University. Each person provided access has a responsibility to protect those systems and the data and information they contain. As such, passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Lakehead University's entire corporate network. As such, all Lakehead University employees, contractors, and vendors with access to Lakehead University systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 PURPOSE

This procedure establishes a standard for creation, handling, and expiry of strong passwords.

3.0 SCOPE

This procedure includes employees, students, contractors, consultants and any other user who has or is responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Lakehead University facility, has access to the Lakehead University network, or stores any non-public Lakehead University information.

4.0 PROCEDURE

4.1 GENERAL

- All system-level passwords (e.g., root, enable, Windows admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the TSC administered global password management system. All accounts with administrative privileges or those with the ability to escalate privileges should also be documented in the global password management system.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. More frequent changes although not mandatory, are recommended.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication. This includes but is not limited to discussions over cellular or radio networks.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

4.2 REQUIREMENTS

- Minimum Length - 8 characters
- Maximum Length - 14 characters
- Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:
 1. Lowercase
 2. Uppercase
 3. Numbers
 4. Special characters such as !@#%&*(){}[]

Note: Some systems do not support special characters

- Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 5.
- Maximum password age - 180 days
- Minimum password age - 2 days
- Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. they can press the CTRL-ALT-DEL keys and select "Lock Computer".
- See section below for guidelines on password construction.

4.3 GUIDELINES

4.3.1 General Password Construction Guidelines

Passwords are used for various purposes at Lakehead University, including user level accounts, web accounts, email accounts, screen saver protection, voicemail password, router and other networking component administrative logins. Since many of the systems we use do not have support for one-time tokens (i.e. dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#%&*()_+|-~`=\ {}[]";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, nor slang, dialect, jargon, or abbreviation
- Are not based on personal information, names of family, etc.
- Passwords should be memorable. For example, create a password acronym based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Poor, weak passwords have the following characteristics:

- The password contains fewer than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "Lakehead University", "lakeheadu", "lakeu" or any derivation.

- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Words concatenated with numbers (e.g. password4you)

4.3.2 Password Protection Standards

Use different passwords for Lakehead University and non-Lakehead University access (e.g. personal ISP account, option trading, benefits, etc.). Where possible, always use different passwords for various Lakehead University access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Keep all of your passwords private; there is no reason to share Lakehead University passwords with anyone, including administrative assistants, secretaries, TSC staff or more particular, any outside organization. All passwords are to be treated as sensitive, confidential University information.

Here is a list of “don’ts”:

- Don't reveal a password over the phone to ANYONE
- Don't put a password in an email message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., “my family name” or song title)
- Don't reveal a password on questionnaires or security forms – no one will ask you for that information legitimately
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them contact the Director of Technology Services Centre.

Do not use the "Remember Password" feature of applications (e.g. Eudora, Outlook, and Thunder Bird).

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to [Technology Service Centre's Helpdesk](#) and change all passwords.

Active security checking may be performed on a periodic or random basis by Technology Service Centre or its delegates. If an account is compromised during one of these scans, the user will be required to change it.

4.3.3 Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.
- should employ current conventions and standards for secure applications (MD5, SSHA, etc.)

4.3.4 Use of Passwords and Passphrases for Remote Access Users

Access to the Lakehead University Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

4.3.5 Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known 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:

"Th3Tr@ffic0nTh34o1WasTerribl3ThisM0rning"

All of the rules above that apply to passwords apply to passphrases.

All SSL certificates in use must employ good passphrases.

4.3.6 Key stores

Some systems rely on key stores to keep passwords and perform other access control. Key stores must be readable only to the accounts that employ it (i.e. the UNIX account under which the daemon runs). Also, key stores must be encrypted with a pass phrase (as above) that is not stored on the system.

5.0 FAILURE TO COMPLY

Any account that fails to comply with this procedure may be suspended by Technology Services Centre without notice.