

- a. All users are responsible to keep their passwords confidential.
- b. Users are responsible for any actions that may be traced to the use of their password.
- c. UCIT personnel will never ask users to divulge their passwords.

4.3 *Minimum Complexity Requirements*

All passwords must have a minimum size of 7 (seven) characters in length and meet at least three of the following complexity requirements:

- Must contain a minimum of 1 upper case alphabetic character.
- Must contain a minimum of 1 lower case alphabetic character.
- Must contain a minimum of 1 numeric character.
- Must contain a minimum of 1 special character.

4.4 *Password Lifetime*

Currently, there are no restrictions on Password Lifetime. However, users are strongly encouraged to change their Passwords at least every ninety (90) days.

4.5 *New, Temporary and Default Passwords*

- a. Passwords must be communicated to the end user in a secure manner and through the use of separate communication channels.
- b. All accounts where new or temporary passwords have been issued must be disabled if the account has not been used within seven days.
- c. All temporary passwords must be changed immediately following their initial use to gain system access.
- d. Under certain circumstances, default user IDs and passwords are shipped with operating systems, hardware systems, applications and other products for use during installation and setup. These default passwords must be changed immediately during, or following their initial use prior to connecting to the University network.

4.6 *Compromised Password Reset*

If any password is suspected to have been compromised it must be changed immediately and reported to the UCIT Support Center.

4.7 *Physical Password Storage*

- a. Passwords must be properly secured at all times.
- b. Passwords for a particular system may be kept in a sealed envelope in a safe or locked cabinet and retrieved only when required.

4.8 **Electronic Password Storage**

- a. Passwords must never be stored in clear text (readable) form in any file or database on any system.
- b. Individual passwords used for automated processes (machine to machine authentication or in macros; batch files; script files and source code) can be stored in clear text provided access is restricted to the process/application associated with the particular use of this account and password. These passwords must not be readable by anyone else.
- c. Passwords may be stored electronically using approved password management applications. A list of approved applications can be found at www.ucalgary.ca/it/infosecurity

4.9 **Electronic Password Usage**

Passwords may not be transmitted to any authentication mechanism or service in clear text. All passwords must be encrypted prior to requiring access to system, services and applications.

Exceptions	5	The CIO can approve exceptions to the above standard. Exception requests shall include detailed descriptions of: <ol style="list-style-type: none">a. Why the proposed solution is being requested rather than following the standard.b. How the proposed solution varies from the standardc. What are the implications for long term management of the variation															
Parent Policy	6	Information Asset Protection Policy															
Related Policies & Standards	7	Information Asset Security Monitoring Policy Information Asset Management Policy Information Security Classification Standard															
History	8	<table><tr><td>Feb 12, 2009</td><td>Patrick Jungles</td><td>Revision</td></tr><tr><td>April 6, 2009</td><td>Patrick Jungles</td><td>Revision</td></tr><tr><td>May 13, 2009</td><td>Dennis Tracz</td><td>Revision ITASC feedback</td></tr><tr><td>Aug 25, 2009</td><td>Patrick Jungles</td><td>Revision/Inc ITASC comments</td></tr><tr><td>Nov 12, 2009</td><td>Crystal Bourgeault</td><td>CIO Approval</td></tr></table>	Feb 12, 2009	Patrick Jungles	Revision	April 6, 2009	Patrick Jungles	Revision	May 13, 2009	Dennis Tracz	Revision ITASC feedback	Aug 25, 2009	Patrick Jungles	Revision/Inc ITASC comments	Nov 12, 2009	Crystal Bourgeault	CIO Approval
Feb 12, 2009	Patrick Jungles	Revision															
April 6, 2009	Patrick Jungles	Revision															
May 13, 2009	Dennis Tracz	Revision ITASC feedback															
Aug 25, 2009	Patrick Jungles	Revision/Inc ITASC comments															
Nov 12, 2009	Crystal Bourgeault	CIO Approval															