Centre for
Heart Lung Innovation
UBC and St. Paul's Hospital

STANDARD OPERATING PROCEDURE

Title:	**7.5 Password Policy**		
Procedure:	**PR-0705(2)**	**Supercedes:**	**PR-0705(1)**
Originator and Date:	**Marilyn Andersen October 24, 2004**	**Effective Date:**	**19April2012**
Review Frequency:	**annually**	**Approved By:**	**The JHRC Privacy Team**
Total Number of Pages: 4			

Revision History		
Date	**Reviewer**	**Summary of revision**
Jan2006	Mark Wilkinson & Wendy Alexander	No details of revisions recorded
Feb2007	Mark Wilkinson & Wendy Alexander	No details of revisions recorded
Feb2008	Byron Kuo, Mark Wilkinson, Joe Comeau	Password expiration changed from 42 days to 6 months. Added info on changing a forgotten password
25Apr2008	Jacqui Brinkman	Revision History table added, replacing "Last Date Reviewed and Reviewer" box Updated UBC weblink, 'B' under references
28April2009	Joe Comeau	Minor edits to procedure bullet 4
19Apr2012	Raquel Park/Joe Comeau	Update "iCAPTURE Centre" to "JHRC"
Aug 2013	Raquel Park/Joe Comeau	Update "JHRC" to "HLI"

1. BACKGROUND

Passwords are used to validate a user's identity to access an information system or service and support accountability and appropriate data management. Please note that the details of this policy are typical of organizations that maintain confidential information. The policy as described is considered best practice and is used broadly in government and industry. It can be argued that research requires an even higher standard.

2. PURPOSE

- To maintain the security and confidentiality of information stored in the electronic files that the Centre for Heart Lung Innovation relies upon to conduct business.
- To provide user-specific accountability for tracking and monitoring the use of information systems and access to data.
- To provide a security framework for the use of electronic authentication and electronic signatures.
- To comply with the ***FOIPPA*** legislation.

3. SCOPE

This policy applies to all systems whose security is managed by the HLI as well as to those from which the HLI relies on and has influence over. These systems include: file servers, application servers, print servers, e-mail servers, Internet gateway, fax servers, database servers, data warehouse servers, report servers, printers, network components and client workstations. All applications which include personally identifiable information or corporate information are included in this policy.

4. POLICY STATEMENT

The allocation of passwords is controlled through a formal management process. Each user will be assigned a unique user account to provide access to the unique resources that they require. All users will be required to sign an agreement to keep personal passwords confidential.

Each user is responsible for managing the confidentiality of, and all activity performed with, their personal password. Similarly, users are forbidden from performing any activity with another user's personal account unless the owner of the personal password is present.

Passwords for HLI access must be unique. Users should not employ passwords that are used on other accounts.

Standards of password complexity and reset cycles will be employed.

5. PROCEDURE

In order to prevent unauthorized access, users MUST NOT:

- Reveal and/or share their passwords to other users, including to any Information Systems team member;
- Write their passwords on any visible media;
- Transfer their passwords electronically unless they are encrypted;
- Leave the computer accessible and in logged-on position while not in attendance.

The Computer Password Policy will be available to all users on the HLI Intranet as well as in the Training Document provided to all new personnel.

In order to minimize the risks associated with unauthorized access, users will be required to change their password as follows:

- The maximum password age is 90 days for users who have access to identifiable research subject/partner information;
- To prevent password recycling, the minimum password age is 1 day, and users will not be able to reuse any of their previous eight passwords;
- User accounts will be locked out after three failed logon attempts within 5 minutes. The failed logon count must be reset by IT Services.

Users are required to select a "strong" password with the following characteristics:

- The password must not contain all or part of the user's account name;
- The password must not be constructed based on personal information (e.g. birthday, first/last name and telephone number);
- The minimum acceptable password length is 8 characters;
- The password is recommended to contain characters from 2 of the following 4 categories:
  - English uppercase characters (A - Z);
  - English lowercase characters (a - z);
  - Base 10 digits (0 - 9); and,
  - Non alphanumeric (For example: !, $, #, or %);
- The password should be easily remembered, so users do not have to write their password down;
- The user must not use the "Remember Password" feature of any software application (e.g. Internet Explorer).
- Forgotten passwords may be changed after correctly answering challenge questions.

Users should report any suspicious and/or inappropriate activity to the HLI Help Desk.

Procedure for Helpdesk access:

1. When support technicians are required to access a user account to provide support or troubleshoot problems, users must either be available in person to log on to their own account or allow the technician to take control of their process remotely rather than providing the technician with the password to their account.

2. In the rare case where a user account must be accessed by IT staff, the IT staff member will reset the password to a pre-expired password and inform the account owner. This will allow the account owner to log on and immediately change the password.

6. REFERENCES

A. Centre for Heart Lung Innovation Research Centre Policies:

- PR-0702: Administrative Security Controls;
- PR-0706: Acceptable Use of Computer Accounts.

B. UBC Policy #104: Responsible Use of Information Technology Facilities and Services (http://www.universitycounsel.ubc.ca/policies/policy104.pdf)

C. CSA ***Model Code*** Principle #7, Safeguards.

D. ***Pattern-based passwords: Easy to remember non-dictionary based passwords*** Craigin Shelton, 21 Aug. 2001 searchsecurity.com.

E. ***Security Is A Business Issue***, a presentation by Charlie Johnson VP Global Business Development Symantec, 2001.