DALHOUSIE UNIVERSITY Health Data Nova Scotia **Passwords Policy**	**Author:** S.Kennedy	**Review Date:** 01.01.2018
	Approved by and date: S.Carrigan / 05.04.2017	**Effective Date**: 05.04.2017
	Version Number: v1.0	***Page 1 of 6***

1. BACKGROUND & PURPOSE

1.1 The use of passwords to prevent unauthorized access to electronic information is one of the basic measures used to protect identities and the security of personal and other information.

2. APPLICATION

2.1 This policy applies to all Health Data Nova Scotia (HDNS) authorized personnel and approved users.

3. DEFINITIONS

3.1 *Approved Users:* Individuals who have been issued an access account, key code or swipe card following the approval of access per the relevant procedures. Approved users may include students, trainees, researchers, health service assessment analysts and other users of the HDNS such as government staff or analysts hired by researchers.

3.2 *Authorized Personnel:* Users who have been authorized to access data at HDNS which includes:

- HDNS staff and contractors (including system administrators/managers, analysts, documentation specialists).

3.3 *NetID*: The unique identifier given to staff and students of Dalhousie University for purposes of accessing Information Technology (IT) services.

3.4 *Password*: A series of numbers, letters and/or characters used to control access to electronic devices, systems, programs or data.

4. POLICY STATEMENT

4.1 An initial temporary password is assigned only after the individual's identity has

been reasonably established.

4.2 The individual will be prompted to change the temporary password after logging on using the existing password.

4.3 Protection of passwords is the user's responsibility. Passwords MUST not be shared with or revealed to anyone else.

4.4 Forgotten or unusable passwords may be reset for a user once there is a reasonable assurance of correct identity.

4.5 Passwords for all systems are subject to the following rules:

- Passwords are unique to user and function. A user with multiple duties and/or projects may have distinct passwords for each function, duty or project. There is no generic or shared login to any system.
- No passwords are to be written, emailed, hinted at, shared, or in any way made known to anyone other than the user involved. This includes supervisors and assistants.
- No passwords are to be shared to "cover" for someone out of the office.
- Passwords cannot include an individual's name, address, date of birth, username, nickname, license plate, or any term that could easily be deduced by someone who is familiar with the user.

4.6 When an employee leaves HDNS, all their accounts are terminated and any system passwords are immediately changed. When users complete a project or when a project is terminated for any reason, user account access is immediately suspended.

4.7 Passwords governed by the Password Policy must meet all the following minimum standards:

- At least 8 characters, including at least three of the following four character types:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Symbols found on your keyboard; a blank space is not permitted but all of the following are: ~@%^&*_={}[]()+;,./<>?# -
- No embedded NetIDs or Banner numbers.
- No embedded sequences of four or more characters of the following types:
  - Repeated characters, such as AAAA or 5555;
  - Alphabetic sequences, such as abcd or DCBA;
  - Numeric sequences, such as 1234 or 4321;

    - Common keyboard sequences, such as QWER or poiu.
- No embedded words from a dictionary of English words or names. Short words of four or fewer characters are permitted.

4.8 Breach of this policy could result in termination of employment or access to HDNS.

5. PROCEDURES

5.1 Users must have a Dalhousie NetID or Project NetID prior to receiving a password.

5.2 Once an authorized personnel or approved user has a Dalhousie NetID, the Systems Administrator will set a temporary password and instruct the individual to change the password in accordance with this policy.

6. ADMINISTRATION

6.1 Accountability

6.1.1 The System Administrator is responsible for providing initial passwords to authorized personnel and approved users and reporting any password violations to the HDNS Manager.

6.1.2 Authorized Personnel and approved users are responsible for protecting passwords and ensuring that their password is not shared or revealed to anyone else.

6.1.3 HDNS authorized personnel and approved users are responsible to report any breach of this policy to the Systems Administrator and the HDNS Manager.

6.1.4 The HDNS Manager is responsible to investigate and address any breaches of this policy.

6.2 Monitoring, Auditing and Reporting

6.2.1 The Systems Administrator provides logs of all HDNS system users and account activity.

6.2.2 Random security audits which log every access attempt on protected data (whether successful or not) of the HDNS system are conducted occasionally by the Systems Administrator.

7. RELATED POLICIES AND OTHER DOCUMENTS

7.1 HDNS Policies and Procedures

- HDNS Data Access Policy
- HDNS Privacy Incident and Breach Policy
- HDNS Privacy Training Policy
- HDNS Security Policy

7.2 HDNS Forms

- HDNS Confidentiality Agreement /Acknowledgment

7.3 Other Documents

- Dalhousie University Secure Facility Policy

Dalhousie University Guidelines for Composing Passwords

Your HDNS user ID, authenticated by your password, permits you to access electronic services that are restricted to the HDNS community. These services are important to you and to the University and must be protected by a password.

Your password should be easy for you to remember, but difficult for anyone else to discover or guess. Don't base your password on personal information; avoid using your spouse's or children's name, the names of pets, birth dates, hobbies, favourite sports, your address or phone number, Social Insurance Numbers, license numbers, etc.

Here are two methods of arriving at a good password:

1. Passwords based on mnemonic phrases are among the most secure and easiest to remember. Start with a line from a favorite song, poem, film, or speech. Take the first letter of each word and keep the punctuation, or pick one or two letters or symbols to represent each word, and then mix in punctuation and numbers that are meaningful to you.

- Example: Take the phrase "*And that's the kind of day it's been*" to create the password **&T'stkodib**
- Example: Take the phrase "*I was 21 when I first visited Paris*" to create the password **Iw21wIfvP**
- Example: The song chorus "*We'll rant and we'll roar...*" combined with the year of the Halifax explosion could become **wr&We'llr17!**

2. Start with a real word, or words, and then modify slightly. But do not rely on simple substitutions, such as replacing the letter O with the number zero, because these are well known to password crackers.

- Take two short *unrelated* words and combine them with special characters or numbers. Example: **Game48keys** or **eye!!wEEk**
- Introduce 'silent' numbers into a real word (you'll need at least one uppercase too). Example: **termin7Al**
- Deliberately misspell a word or phrase (you'll still need at least one number and uppercase). Example: **37ChokLuts**

Regardless of the method you use, choose passwords that you can remember that will be difficult for even those who know you to guess. Dalhousie enforces rules that help make your password stronger.

Those rules include a minimum length of 8 characters, no embedded dictionary words, mixture of alphanumeric and special characters, etc. Password change pages have a help section that explains this in more detail.

Don't use any of the example passwords shown on this page!

Now that you have a password ...

- Passwords must be kept secret and must not be shared with anyone.
- It is best to remember your password and not write it down anywhere. If you must write your password down, make sure you keep it in a safe place – such as in your wallet. Never store it near your computer or in a file on your computer.
- Change your password immediately (contact the HDNS System Administrator) if you suspect that someone may have guessed it.
- Use your new password immediately after changing it to help make it stick in your memory.