DALHOUSIE UNIVERSITY
Inspiring Minds

Information Technology Policy

5.2.1 Passwords

Policy

Area: 5.2 Security	**Date Issued:** 2006 July 24
Title: 5.2.1 Passwords	**Last Revision Date:** 2011 October 19
Issued by: Assistant Vice-President/CIO, ITS	**Approved by:** Assistant Vice-President/CIO, ITS

Purpose

Passwords, as normally used, are the minimum level of electronic security for protecting identities and the security of personal and other information. Passwords must be chosen and used with care in order to give reasonable assurance of that protection.

Policy Statement

1. An initial password may be assigned to a user only after that user's identity has been reasonably established.
2. A user must be allowed to change his or her own password after logging on using the existing password, provided the existing password has not been made unusable.
3. Passwords the user has previously used may not be reused within the time specified in the attached procedures.
4. Passwords:
   - must be resistant to brute-force attacks; and
   - must not be forced to be more complex or difficult to use than is required to meet changing security requirements.
5. Protection of passwords is the user's responsibility. *Personal* passwords must not be shared with or revealed to anyone else. *Project* passwords may only be shared among those identified by the project leader as having a legitimate need to know the password.
6. Forgotten or unusable passwords may be reset for a user once there is a reasonable assurance of correct identity, but this level of assurance will generally be more strict than that required for the initial password. A copy of the new password must not be kept by anyone except the legitimate personal user or project users.

Applicability of this Policy

This policy applies to passwords used for common services and associated with the following authentications:

- Systems using Dalhousie NetID authenticated via the Enterprise Directory service, for example MyDal.
- Other systems using NetID and synchronized with the Enterprise Directory password

This policy sets base requirements for passwords. Some situations, such as privileged access to servers, may have more stringent requirements and will be the subject of separate policies.

Procedures

Setting the initial password

Personal accounts

When a NetID is initially assigned there is no associated password (i.e. the password is reset and the NetID is not functional). The user to whom the NetID has been assigned may set the initial password by supplying their Banner ID number and their birth date. Users are told their Banner ID number by non-electronic means when they are first registered as students, or first employed, or when a relationship is first established.

Guest accounts

The initial password for a guest account will be automatically generated and given to the user who has authorized the account (usually a faculty or staff member).

Project accounts

An initial password is assigned by Networks and Systems when a project account is created. This password is securely transmitted to the project leader. The password should be set to expire within 1 week.

Changing a password

Users will be provided with a secure web page that can be used to change their password at any time. Knowledge of the NetID and the currently usable password is sufficient to make the change.

Password re-use

New passwords must be checked to ensure they have not been used for this NetID within the past 12 months.

Password Strength

Passwords must be checked for compliance with the attached standard before they are accepted.

Forgotten or unusable passwords

Personal accounts

Self Service: Users may reset (make unusable) their own password by one of the following:

- A valid login to DalOnline where they will be presented with a function that will reset their NetID password; or
- Specifying their NetID, Banner ID, and EM email address to a web page, which will result in a limited lifetime URL that can reset the password being sent to that email address; or
- Specifying their NetID and Banner ID to a web page, which will result in a limited lifetime URL that can reset the password being sent to the postal address on record.

Assisted Service: Authorized staff may reset (make unusable) a forgotten password once the identity of the user is reasonably established. The user may then set a new password by knowing their Banner ID number and their date of birth as recorded in Banner.

- A user requesting a password reset must be identified by providing their Banner ID number and at least one of the following:
    - Appearance in person and presentation of an acceptable photo ID; or
    - A FAXed or emailed copy of an acceptable photo ID together with a signed request for the reset specifying the user's Banner ID and NetID:

- An acceptable photo ID is one of the following valid documents:
    - Dalhousie ID card (the Dalhousie ID card may be expired if the user does not have a current affiliation with Dalhousie that requires an ID card, e.g. alumnus); or:
    - Passport; or
    - Canadian or US driver's license with photo.

- Only the following persons will be considered for authorization to reset users' passwords. This authorization will expire in no more than 12 months and renewal must be requested by the person's dean or senior director and accepted by the Director or Associate Director of Networks & Systems, and audited by the ITS Information Security Manager. This authorization will be withdrawn when the person's status changes or on any breach or suspected breach of these procedures.
    - ITS Directors and Managers
    - ITS Help Desk staff
    - ITS workgroup managers
    - Regular full time user support staff in Faculties and departments

- A log entry of all password resets will be maintained for at least two years. The log will include the affected NetID, a log of the identifying information supplied by the user, a timestamp, IP number or other identification of the workstation used, and identification of the person carrying out the reset.

Guest accounts

Passwords for guest accounts may be changed by the guest account user but cannot be reset.

Project accounts

A forgotten or expired password may be changed by Networks and Systems on the request of the project leader. The project leader's identity will be established as above. The new password should be set to expire within 1 week.

Exceptions

Exceptions to these procedures may only be made on the written direction of the Assistant VP/CIO, ITS.

Standards

Passwords governed by the Password Policy must meet all of 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.

Guidelines

Your NetID, authenticated by your password, permits you to access electronic services that are restricted to the Dalhousie 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 (at https://password.dal.ca) 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.

Definitions

authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. For example, it is the process of deciding whether the person attempting to use a NetID is the person to whom that NetID was assigned.

Banner ID

A user's Banner ID is the identification number assigned to a user by the University's central administrative system. It is also known as a Dalhousie ID, a Student ID, or an employee ID and has the form of the letter 'B' followed by 8 digits.

brute-force attack

A brute-force attack is an attempt to determine a password by trying all possible combinations. For example, a 6 digit PIN consisting only of the digits 0-9 can be guessed in at most 1,000,000 tries. Even strongly encrypted passwords can quickly fall to brute force attacks if the attacker has a copy of the encrypted password and if the password is not well chosen.

EM address

An EM address is one of the non-Dalhousie email addresses recorded in Banner as 'Personal' email addresses.

Enterprise Directory

Dalhousie's Enterprise Directory contains digital information that, among other things, facilitates the authentication process. Managed by ITS it is the only authoritative directory for electronic authentication purposes at Dalhousie. It may take the form of OpenLDAP, Active Directory, or other some technology in the future.

guest account

A guest account is a short-duration account with strictly limited privileges that is designed to be used by visitors and guests at Dalhousie. Guest accounts may be generated by any faculty or staff, who then become responsible for the use of that account.

password

A password is a string of characters that is used in association with a username/identifier to authenticate a user to an electronic application. The password should only be known to the user.

project account

A project account is an account and associated NetID that is not associated with any one person, but rather with a group of persons for a particular purpose. A project account to be used for a conference website is an example. Although several people may access the account, one person is ultimately responsible for its use.

personal account

A personal account is an account and associated NetID associated with one person only. Most email accounts are examples.

Related Documents

Official NetID password page: https://password.dal.ca

Revision History

2011 October 19	updated Procedures to match current practices
2009 October 13	changed from 'UCIS' to 'ITS'
2008 January 09	updated language about who can do resets, allowed emailed photo ID, allow expired ID in some cases
2006 July 24	initial approved version