University Information Security Standard

Complete Policy Title:
Identity and Access - Password Standard

Policy Number (if applicable):
IS-09-PASS

Approved by:
Chief Information Officer

Date of Most Recent Approval: (annual review)

Date of Original Approval(s):

Supersedes/Amends Policy dated:
n/a

Responsible Executive:
Chief Information Officer

Enquiries:
IT Security (c-it-security@mcmaster.ca)

DISCLAIMER: *If there is a discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails.*

TABLE OF CONTENTS

IDENTITY AND ACCESS STANDARD

INTRODUCTION

Passwords are a common means of authenticating the identity of a customer before authorizing access to a resource or service. Quality passwords provide an essential layer of defense in securing McMaster University assets from unauthorized use or access.

Purpose

1. It is the responsibility of all University Constituents to exercise appropriate care when creating and securing their passwords.

2. Failure to properly manage passwords, such as sharing or choosing weak passwords, may lead to unauthorized access to personally identifiable information, disclosure of intellectual property, unauthorized disclosure of University information, reputational damage and/or monetary loss.

Scope

3. This standard applies to any University Constituent responsible for any account that is used to access the University information or resources, regardless of their affiliation with, or function within the University.

4. This standard is extends to any computing device or service that handles University information or is used to process or store University resources. This standard is applicable regardless of the physical location of the device or service, including internet or “cloud” based services.

Definitions

5. University **Constituents** are individuals that have an existing relationship with the University, including but not limited to adjunct professors, affiliates, alumni, external contractors, faculty, graduate students, guests, librarians, partners, postdoctoral fellows, retirees, staff, undergraduate students, visiting professors, visitors, and volunteers.

6. **Accounts** are the full record of activity, communication, and content accessible to a Constituent who is a customer of a service. This includes, but is not limited to, email mailboxes, home directories, computer profiles, telephone voicemail, and University managed, sponsored, or branded social networking profiles.

7. The **account holder** is the individual for whom the account was provisioned, and the individual who is responsible for the account. A **delegate** is an individual for whom the account holder has authorized and arranged access to use the account.

8. **Credentials** are the mechanism used to authenticate an individual in order to provide access to an account. Credentials usually consist of a user identifier (e.g., MacID) and a password.

9. Accounts with **elevated privilege** are those that are used to configure service and resource settings, and the access privileges of other users. Such accounts include, but are not limited to, *administrator*, *root,* and service principal accounts. In most cases an account with elevated privilege is a named account to which administrative privilege or role(s) have been granted.

10. A **role** is the set of connected privileges that are assigned to credentials to enable the owner to perform their functional responsibilities. Examples of roles include, but are not limited to, *administrator*, *power user*, *user*, or *guest*.

11. A complete glossary of definitions can be found in the ***Information Security Glossary***.

REQUIREMENTS

Password Use

12. All McMaster University technology assets must be protected by password controls where the technology exists. In the absence of password controls described by this standard, compensating controls must be implemented.

Constituent Rights, Privileges, and Responsibilities

13. Each constituent will be assigned unique credentials with which to access University managed technology resources, services, and accounts. These credentials must not be shared, even with a supervisor or among co-workers. It is the responsibility of each constituent to ensure that their assigned credentials comply with this standard. It is the responsibility of each constituent to protect and prevent the misuse of the credentials that have been assigned to them.

14. Credentials will not change if a constituent changes roles. If the credential unique identifier (i.e., account name, user name, or MacID) does not adequately identify the account holder, they are encouraged to use an alias. Reasonable requests to change credential unique identifiers will be accommodated.

15. Credential owners must choose strong passwords that comply with the password complexity requirements defined below, and must use a unique password for every account they own. (i.e., every account they log into, internal or external to the University, must have strong and unique passwords).

16. Credential owners must change their password(s):

    a) at least once every 365 days;

    b) immediately after the first time it is used to access a new account, or when the password has been reset by a third party;

    c) when there is any indication of possible system or password compromise; in addition such incidents must be reported to the appropriate authority.

17. Passwords should never be written down or stored in a format that is human readable. Credential owners must encrypt passwords for storage, and this should only be done for backup, disaster recovery, and business continuity purposes.

System Administrator Responsibilities

18. System administrators, or individuals responsible for creating accounts or assigning roles and access entitlements, must establish secure processes and procedures for managing customer passwords:

    a) These processes must create strong and unique temporary passwords, and distribute these to customers in a secure manner which assures the confidentiality and integrity of the password. A secure procedure must be used to verify the identity of a customer prior to issuing or resetting a password.

    b) Customer password complexity requirements and first logon password reset must be enforced on all systems where the technology permits.

Accounts with Elevated Privilege

19. Accounts with elevated privileges have greater impact than most standard accounts at the University. Extra care must be taken in the management of passwords for credentials used to access such accounts.

20. Default manufacturer and /or vendor passwords must be changed before connecting new systems to the network.

Password Complexity Requirements

21. Passwords must be a minimum of eight (10) characters in length.

22. Password must include character(s) from at least three of these four character sets:

a) Uppercase letters A, B, C, ... ,Z

b) Lowercase letters a, b, c, ...,z

c) Numerals 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

d) Symbols ~ ! @ # $ % ^ & * ( ) _ + ` - = { } |] [\ : " ; < > ? , . /

23. Password must *NOT* contain your account name or recognizable parts of your full name.

24. Password must be unique; the previous five (5) must NOT be used when a password is changed.