McMaster University

University Policy

Complete Policy Title: **Information Security Policy**	Policy Number (if applicable): **IS-00**
Approved by: **President and Vice Presidents**	Date of Most Recent Approval:
Date of Original Approval(s):	Supersedes/Amends Policy dated: **Use of McMaster Computers and Networks (Nov 2010)** **Information Security (Nov 2010)** **Electronic Communications (Nov 2010)**
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

INFORMATION SECURITY POLICY

INTRODUCTION

1. In order to maintain business continuity and the University's reputation, it is critical to protect the confidentiality, integrity, and availability of:

   a) information that supports the operation of the University

   b) personally identifiable information, including health information

   c) intellectual property and copyrighted information

Purpose

2. The purpose of this Policy is to provide direction for the appropriate use of computing resources, including communication and collaboration services and accounts.

Scope

3. This Policy applies to all University Constituents who are able to create and share information using University computing resources, and to any person or organization that handles University information and data regardless of their affiliation with or function within the University.

Definitions

4. 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.

5. A **computing resource** is any type of computer that is connected to the University data or telephony network. This includes but is not limited to servers, workstations, laptops, mobile devices, network appliances, telecommunication and teleconferencing devices, printers, automation hardware, and industrial control systems.

6. **Communication and collaboration services** are defined as digital technologies with which Constituents collaborate, communicate, share opinions, files, or other information. Services may include, but are not limited to: email, network storage, telephone, instant messaging, University managed, sponsored, or branded social networks, cloud services, printers, and online comments. The **service owner** is the department head who is accountable for the service, and computing resources required to provide the service, within the organization.

7. **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.

8. 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. A **sponsored account** is any account for which the holder is not identifiable by the account name. Examples of sponsored accounts include, but are not limited to, shared accounts, role based accounts, generic accounts, and guest accounts.

9. **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.

10. **Information Security enterprise standards** are general statements outlining technical requirements that must be met in order to remain in compliance with this Policy.

11. **Canadian Anti-Spam Legislation (CASL)** protects Canadians from the threats related to digital communications, including spam, phishing and malware. (https://www.mcmaster.ca/privacy/casl/ and http://crtc.gc.ca/eng/internet/anti.htm)

12. The **Canadian Copyright Modernization Act (CMA)** protects copyright owners from inappropriate access to their materials, and defines the responsibilities and liabilities of internet service providers. (http://laws-lois.justice.gc.ca/eng/annualstatutes/2012_20/FullText.html)

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

POLICY: ACCEPTABLE USE OF COMPUTING RESOURCES

Intended Use

14. University computing resources, services, and accounts are intended for use by University Constituents for activities outlined within and supported by the mission and vision of McMaster University. Such activities include, but are not limited to education, research, health care, University business, student life, community engagement, health and safety, and public service.

Incidental Use

15. It is accepted that Constituents may use University computing resources, services, and accounts for incidental personal purposes. Constituents are required to exercise good judgment and conduct themselves professionally regarding incidental personal use of University accounts. Use of University accounts for the benefit of a private business or commercial enterprise is restricted by existing University policies, including but not limited to the ***Conflict of Interest Policy for Employees***, ***Code of Student Rights and Responsibilities***, and ***Statement on Conflict of Interest in Research***.

Constituent Rights, Privileges, and Responsibilities

16. Constituents are responsible for observing all applicable laws, University policies, and contractual agreements while using computing resources, services, and accounts.

17. Constituents have the right to access only the accounts, information, and computing resources to which they have been granted explicit authorization, or to which authorization is implied by the disposition of the account, information, or resource. Constituents are responsible for safeguarding computing resources, accounts, and information in their care.

18. Each Constituent will be assigned unique credentials with which to access University managed 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 Policy and related Standards, including the ***Password Standard***. It is the responsibility of each Constituent to protect and prevent the misuse of the credentials that have been assigned to them.

19. 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.

20. Account holders have the authority to delegate access to their account as reasonably required within their role at the University. Delegate access should be granted using unique credentials rather than shared common credentials; exceptions may be made where there are technical constraints preventing delegation to another unique account. Delegates are required to adhere to

the same standards of acceptable use as they would in any account which they hold or to which they have access. Account holders retain responsibility for the actions of their delegates.

21. Constituents are responsible for managing the content of their account(s). Any backups or redundancy provided by the service provider is in support of disaster recovery and business continuity only. There may be limitations on the ability for technical administrators to recover content that has been deleted. Modification and deletion of content should be undertaken responsibly and in accordance with legal and record retention policies.

22. Constituents are encouraged to use alternatives to shared accounts, such as electronic distribution lists, contact groups, delegation, aliases, etc. Where shared accounts are necessary, they should not have active credentials related to them; Constituents should access the shared account using their unique credentials. All shared accounts must have an explicitly identified holder.

23. Electronic distribution lists and contact groups must have an explicitly identified holder. The holder may delegate authority to send messages to list members. The holder and their delegate are responsible for all content sent using the electronic distribution list, and for ensuring that the list is not used to send unsolicited or inappropriate messages. Messages sent using electronic distribution lists must comply with ***Canadian Anti-Spam Legislation (CASL)***. List holders are responsible for maintaining the list membership, and offering a mechanism by which members can unsubscribe from the list where applicable.

24. Constituents are responsible for reporting violations of this policy, and known information security events, incidents or breaches in accordance with the ***Information Security Incident Reporting*** procedure. Breaches of personal information must be reported without delay to the University Privacy Officer.

Information Classification

25. Information that is transmitted or stored using University computing resources, services, and accounts must be handled in accordance with the ***Information Classification Matrix***, in order to maintain appropriate confidentiality, integrity and availability. Information must be re-classified when necessary during its lifecycle to ensure it is appropriately handled and protected. Where possible, information should be labelled to promote appropriate handling and protection.

26. Constituents must comply with the University ***Privacy Governance and Accountability Framework*** while using computing resources, services, and accounts. Faculties, research units and groups, departments, and business units should:

    a) Use internally managed services to handle information;

    b) Assess the risk of sharing information with external services and accounts;

    c) Create standard operating procedures to supplement this Policy, and mitigate risks to sensitive information; and

d) Educate users on their responsibilities and liabilities.

27. All unauthorized or accidental disclosures of information classified as confidential or restricted must be reported to the University Privacy Office (University Secretariat).

POLICY COMPLIANCE

28. The University reserves the right to monitor service and account activity, excluding content, and to audit computing resources on the University data and telephony networks in order to ensure compliance with this Policy. All violations of this Policy will be handled according the "**Policy Violations**" section below.

Breach of Acceptable Use

29. Constituents are prohibited from accessing another individual's account without appropriate authorization.

30. Constituents are prohibited from using services and accounts to access, read, copy, delete, or use University data, information, or resources without authorization. Intentional or involuntary unauthorized release of confidential information is considered a breach of confidence and a violation of this Policy.

31. Constituents are prohibited from engaging in activities that prevent or impede the ability of others to exercise their rights and privileges. This includes, but is not limited to:

    a) the transmission of unsolicited or malicious messages, or installation of unwanted or malicious software, including those defined by the ***Canadian Anti-Spam Legislation (CASL)***;

    b) accessing copyrighted material to which they are not authorized, including that defined by the ***Copyright Modernization Act (CMA)***;

    c) limiting or denying access to services and / or accounts without authorization; and

    d) unauthorized or unwarranted monitoring or surveillance of computing activities.

Service Owner Responsibilities

32. Service owners are responsible for ensuring that their service is configured in compliance with this Policy and are responsible for information technology security within the service.

33. Service owners are responsible for reporting privacy breaches to the University Privacy Office. Known information technology security incidents must be reported to the UTS IT Security team. Suspected and potential information technology security incidents should be reported to the UTS IT Security team.

34. Service administrators and technical administrators will not access Constituent accounts without proper authorization. Where the technology exists to control accounts or the devices upon which accounts are accessed, such technology will only be employed when necessary to remediate violations of this Policy, and will not be employed without notifying the Constituent, after consultation with the University Privacy Officer. Unauthorized access by an administrator will be investigated by the Chief Internal Auditor.

35. Access to an account by someone other than the account holder, or delegate, will be provided upon presentation of a legal search warrant or subpoena. Access may also be provided in the event of imminent physical threat; under such circumstances there must be reasonable belief that access to the account is required in order to prevent harm to one or many individuals.

36. For business continuity purposes, and other legitimate business reasons, it may sometimes be necessary for someone other than the account holder or delegate to access an account. Examples could include termination of employment, sudden leave of absence, or fraud.

    a) Access to staff and sponsored accounts must be authorized by the appropriate Vice-President, or in their absence, the authorized delegate or the Vice-President Administration.

    b) Access to faculty accounts must be authorized by the Provost / Vice-President Academic, or in their absence, the authorized delegate or the President.

    c) Requests for access to an account by someone other than the account holder, or a delegate, should be reviewed and approved by the University Privacy Officer. The Privacy Officer, at their discretion, may recommend administrative, technical, or physical constraints to access. For example, the Privacy Officer may recommend that access be granted for less time than requested, that access logging be enabled for the duration of access, or that access be monitored by another party.

    d) Service providers will be responsible for verifying that access constraints are applied appropriately, and that access is properly revoked.

    e) Account holders will be notified by the authorizing VP as soon as possible without compromising any investigation.

37. Faculties, research units and groups, departments, and business units which oversee or manage an information technology function, whether internal or external, are responsible for securing the information and technology under their responsibility. To this end, they must:

a) Assure that computing resources, services, and accounts in their area are in compliance with this Policy and related Standards;

b) Identify and communicate with owners of data that is stored or processed on computers in their area; and

c) Report incidents of known information technology security breaches to the UTS IT Security team, and to the University Privacy Officer when personal information is involved.

Policy Violations

38. All potential violations of this Policy will be investigated by the appropriate internal authority, and may result in disciplinary actions as per relevant University policies.

39. All potential violations of this Policy could result in the removal of access to services and account privileges for the violator for the duration of the investigation or as directed by the appropriate internal authority.

40. Information technology security incidents that violate any of the above listed policies or legislation is considered violations of this Policy and will be escalated to the internal authority responsible for the policies and/or legislation. For example, violations of this policy that involve systems used to process payments will be escalated to the CFO, or appropriate delegate. Violations may be escalated to external authorities, such as police forces or the Canadian Radio-Television and Telecommunications Commission (CRTC), at the discretion of the internal authorities.

Related Policies and Legislation

41. This document is to be read in conjunction with relevant policies, statements, regulations, and legislation, including:

a) *Code of Student Rights and Responsibilities*

b) *Code of Conduct for Faculty and Procedure for Taking Disciplinary Action*

c) *Statement on Conflict of Interest in Research*

d) *Privacy Governance and Accountability Framework*

e) *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS2)*

f) *Freedom of Information and Protection of Privacy Act (FIPPA)*

g) *Personal Health Information Protection Act (PHIPA)*

h) *Personal Information Protection and Electronic Document Act (PIPEDA)*

i) *Canadian Anti-Spam Legislation (CASL)*

j) Copyright Modernization Act (CMA)

k) Payment Card Industry - Data Security Standard (PCI-DSS)

l) Ontario Human Rights Code

m) Criminal Code of Canada