LU Electronic Services Acceptable Use Policy

Office of Administration:	Department of Information Technology
Approval Authority:	VP Finance and Administration
Approval Date:	Subject to final approval
Last Review:	February 6, 2024
Next Review:	February 2028
Review History:	October 2013, January 2015, September 2016, January 2018, February 2024

1. Purpose

The purpose of this policy is to ensure acceptable use of Laurentian University's ("the University") electronic services and devices.

2. Scope

2.1 This policy applies to all users of LU IT Services (Appendix A), including students, faculty, staff, guest users and affiliates, partners and organisations that acquire LU IT services; and, this policy applies to Laurentian affiliates (eg. partners, retirees including retired professor emeritus, contractors etc.) The scope includes:

2.1.1 Respecting all federal and provincial laws and prohibiting illegal activities,

2.1.2 A process for initiating, reviewing, approving IT policies,

2.1.3 IT development and maintenance,

2.1.4 Delivering properly working electronic services (see Appendix A for list of applications),

2.1.5 The proper operation and conduct of the university in relation to electronic services.

3. Definitions

3.1 Confidential and Personal Information: refers to information that may cause harm to the University, its student, faculty, staff or other entities or individuals if improperly disclosed, or that is not otherwise publicly available.

Confidential and personal Information example include, but are not limited to:

-A trade secret, intellectual property or financial, commercial, scientific or technical information;

-Information where the disclosure could reasonably be expected to prejudice the economic interests of the University or another institution

-Positions, plans, procedures, criteria or instructions to be applied to any negotiations carried on or to be carried on by or on behalf of the University

-Plans relating to the management of personnel or the administration of the University that have not yet been put into operation or made public

-Information regarding employees, including payroll information and staffing information;

3.2 **Personal Information**: refers to any recorded information about an identifiable individual including but not limited to:

-information relating to race, national ethnic origin, colour, religion, age, sex, sexual orientation or marital family status of the individual,

-information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

-any identifying numbers, symbol, or other particular assigned to the individual,

-the address, telephone number, fingerprints or blood type of the individual,

-the personal opinions or views of the individual except where they relate to another individual,

-correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

-the views or opinions of another individual about the individual, and

-the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual" *Freedom of Information and Protection of Privacy Act*, RSO 1990, chapter F.31.

3.3 **LU ID or Credentials**: means one's username and password that give access to the University's electronic systems;

3.4 **Electronic Devices**: includes but is not limited to desktops, laptops, tablet computers, cell phones and other personal digital assistants (PDA).

3.5 **IT Services**: consists of email, storage, business applications, collaborative applications, teaching & learning, research and administrative systems as defined in Appendix A.

3.6 **Federal Anti-Spam Legislation**: an Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the *Canadian Radio-television and Telecommunications Commission Ac*t, the *Competition Act,* the *Personal Information Protection and Electronic Documents Act* and the *Telecommunications Act* (S.C. 2010, c. 23)

3.7 **Deliberate Violation**: A recorded or observed action where a change of behaviour in our systems would trigger a manual action or a notification from a monitoring system (or a ticket).

3.8 **Public Area**: A public area means any indoor or outdoor area that is open to the Laurentian Community (per section 2.1) for public use.

3.9 **Inappropriate and Offensive Act**: An act, be it a comment or conduct, that disparages or demonstrates hostility or aversion towards any person that could reasonably be perceived as disruptive, disrespectful, offensive, or inappropriate.

4. Policy Statement

4.1 The University recognizes its obligation to protect personal information, the intellectual property and access rights of the University users.

4.2 Should work performed by IT for diagnostic purposes and/or maintenance require access to individual files or data that results in a violation of personal information, the intellectual property of access rights, the AVP Information Technology shall report the incident to the Office of the General Counsel.

4.3 Should work performed by IT for diagnostic purposes and/or maintenance uncover information in violation of FIPPA the AVP Information Technology shall report the information to the Office of the General Counsel.

4.4 Research material and intellectual property stored on LU systems or on a cloud system managed by LU, will be treated in accordance with the collective agreement.

4.5 Except for IT diagnostic or maintenance work, access to electronic records can only be accessed when the University's General Counsel declares an exceptional circumstance.

4.6 To the extent this policy conflicts with the provision of any collective agreement, the collective agreement provision shall prevail.

5. LU ID Use and Technology Services

5.1 It is the policy of the University to provide quality access to its electronic systems to those who have a legitimate LU ID and visitors using Laurentian's services (see appendix B for Prohibited uses of LU IT Services).

5.2 Electronic services provided by the University for use by faculty members, employees, students, and other members of the University community are the property of the University, and are intended to be used in a manner that is consistent with the University's mission, and the University's standards of honest and responsible, ethical, professional conduct and consistent with all University policies, guidelines, and does not cause harm to the University.

5.3 The University will onboard a user when the user is approved by:

5.4.1 the Registrar for students;

5.4.2 the HR department for all staff and faculty.

5.4 The University will offboard a user when the user has separated permanently from Laurentian University:

5.4.1 A student will be off-boarded by Registrar less than 18 months after:

- a student graduates, or,
- deemed inactive, or,
- has withdrawn its relationship to LU, either voluntarily or was expelled.

5.4.2 Staff and Sessionals will be offboarded by HR on a date defined by HR for the following reasons:

- Deceased,
- Resignation,
- Retirement, or,
- Termination.

5.4.3 Full time faculty members that retire or that have the emeritus designation will retain a modified level of IT services as described in Appendix D.

5.4.4 The content of a user's Laurentian account(s) will be deleted by IT after 10 months of inactivity, after offboarding, for all members except for LUAPS members and Senior Leadership (retained for 10 years).

5.4.5 Except when retention is authorised by Human Resources, the Office of the General Counsel or by the Registrar.

5.5 Then University IDs and passwords cannot be reused externally and outside of the University official systems per Appendix A.

6. Roles and Responsibilities

6.1 The AVP Information Technology is responsible for upholding IT policies, and promoting continued policy development at LU, and approvals of new and revised standards or guidelines with the IT Governance Executive Team.

6.2 IT Governance comprises of:

- 6.2.1 IT Strategy Governance led by the AVP IT;
- 6.2.2 IT Data Governance led by the Director of Business Applications;
- 6.2.3 IT Security Governance led by the Director of Portfolio; and,
- 6.2.4 IT Project Governance led by the Director of Portfolio.

6.3 IT Governance is overseen by the IT Governance Executive Team. The IT Governance Executive Team consists of the AVP Information Technology, the Vice-President Finance and Administration, the Provost and Vice-President, Academic and the Vice-President Research.

6.4 Responsibility of all LU ID holders

- 6.4.1 It is the responsibility of the ID holder to immediately notify the Office of the General Counsel and IT department of any unauthorised use of user credentials (passwords, usernames or multi-factor tokens) by communicating with the IT Service Desk (it@laurentian.ca or x.2200).
- 6.4.2 Electronic device protection:
  - 6.4.2.1 All electronic devices with confidential and or personal information must be password protected and have an inactivity time-out to auto-logoff within 30 minutes of inactivity or non-surveillance.
  - 6.4.2.2 Passwords cannot be shared with other users.
  - 6.4.2.3 All removable electronic storage devices containing confidential and or personal information must be encrypted by IT per the Policy on Managing Confidential Digital Information.
  - 6.4.2.4 The loss or theft of devices and/or unauthorised access to electronic devices and services must be reported to the Office of the General Counsel and the AVP Information Technology immediately.

6.5 If the University suspects a violation of this Policy, the University mitigation process may be initiated (See Appendix C for the Mitigation Process).

7. Electronic Monitoring of Compliance with this Policy

7.1 To ensure information and systems security, the IT department electronically monitors the use of our systems by University faculty, staff, contractors or agents engaged by a department or employee.

7.2 The IT department does so through audit trails of access to our electronic systems and regular reviews of the audit trails to ensure compliance with this Policy and security of the information we hold.

7.3 Review of audit trails is strictly limited to systems administrators on the basis of need-to-know.

7.4 To learn more about electronic monitoring of Laurentian University information systems, refer to the Policy on Electronic Monitoring.

Appendix A - LU Electronic Services

The University's IT Services consist of email, storage, business applications, collaborative applications, teaching & learning, research and administrative systems.

The full list of applications can be found here:
https://my.laurentian.ca/empl/en/learning?article=46105473 (EN)
https://my.laurentian.ca/empl/en/learning?article=46105475 (FR)

Appendix B - Prohibited Uses of LU IT Services

Laurentian University does not allow improper use of electronic services, including:

a) sharing password(s);

b) attempting to infringe on Copyright material under the Criminal Code of Canada;

c) attempting to circumvent any security or resource management measures;

d) generating or facilitating unsolicited commercial email ("spam"). Such activity includes, but is not limited to:
   i. sending emails in violation of the federal anti-spam legislation, the Canadian Anti-Spam Legislation, or any other applicable anti-spam law;
   ii. imitating or impersonating another person or their email address
   iii. creating false accounts for the purpose of sending spam data
   iv. mining any web property (to LU) to find email addresses
   v. sending unauthorised mail via open, third-party servers
   vi. sending an electronic message such as emails to users who have requested to be removed from a mailing list;

e) selling, exchanging or distributing to a third party the email addresses of any person without such person's knowledge and continued consent to such disclosure;

f) sending unsolicited emails to significant numbers of email addresses belonging to individuals and/or entities with whom you have no pre-existing relationship;

g) sending, uploading, distributing or disseminating or offering to do the same with respect to any unlawful, defamatory, harassing, abusive, fraudulent, infringing, obscene, unlawful pornographic, discriminatory, hate-motivated material or otherwise objectionable content;

h) intentionally distributing viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature;

i) conducting or forwarding pyramid schemes and the like;

j) transmitting content directly to a minor and that may be harmful to them;

k) attempting to interfere with the ability of others to use the network or other commonly shared technology;

l) impersonating another person (via the use of an email address or otherwise) or otherwise misrepresenting oneself or the source of any email and of other electronic services;

m) illegally transmitting another's intellectual property or other proprietary information (LU and others) without such owner's or licensor's permission;

n) attempting to discover or disclose confidential and or personal information stored on University computing facilities;

o) using LU mail to violate the legal rights (such as rights of privacy and publicity) of others;

p) promoting or encouraging illegal activity;

q) interfering with other LU users' enjoyment of all LU services;

r) creating multiple user accounts in connection with any violation of this Policy or creating user accounts by automated means or under false or fraudulent pretences;

s) selling, trading, reselling or otherwise exploiting, for any unauthorised commercial purpose or transfer, any LU account;

t) modifying, adapting, translating, or reverse engineering any portion of the LU services where it might impact business continuity or the performance of services;

u) reformatting or framing any portion of the web pages that are part of the LU service;

v) using any LU services in connection with illegal peer-to-peer file sharing;

w) selling, exchanging or distributing products or services for solely personal benefit and at no benefit to LU;

x) inappropriate, offensive or pornographic use within a public area where others can view material on the computer screen or other electronic devices and can view the person viewing the inappropriate, offensive or pornographic material.

y) exploitation of vulnerabilities in hardware or software for malicious purposes;

z) using a personal email (non-LU email) or other digital means to compromise (directly and indirectly) this policy; and,

aa) any action or activity in violation of a University policy, including but not limited to the Policy on Respectful Workplace, Learning Environment, the Student Code of Conduct, the IT Code of Conduct (for IT personnel), the Employment commitment to Laurentian University and others.

Appendix C - Mitigation Process upon Violation of this Policy and Appeal Process

C.1 When misuse is suspected

C.1.1 If the University reasonably suspects violation of this Policy, the University is authorised to:

a) conduct an examination of a person or person's electronic files, programs or tape, which examination may not be limited to the physical parameters of files;

b) temporarily withdraw a person or person's electronic access privileges if further investigation is warranted, but only after giving notice of the suspension and after specifying a plan of investigation.

C.2 When misuse is confirmed

C.2.1 If the University determines that an individual or a program initiated by an individual has deliberately violated this Policy, the University may:

a) invoke the IT Breach Process;

b) invoke actions from the Office of the General Counsel;

c) withdraw that person's access to the electronic facilities and resources;

d) commence a civil action if the misuse has caused harm to the University or any member of its community, and, if criminal act or intent is suspected;

e) contact the police, who may prosecute pursuant to the Criminal Code.

C.3 Appeal Process

C.3.1 Any appeal of the withdrawal of access (credentials) must be addressed to Laurentian’s VP Administration in person, by telephone or by LU email (vpadmin@laurentian.ca)with the subject line of APPEAL AUP.

Appendix D - IT Services for Emeritus and Retired Full Time Faculty Members

Retired faculty members (including emeritus) will retain their Laurentian ID and access to the following IT services:

- Retain same Laurentian ID;
- Multi-factor authentication and Cyber Sec training;
- Google for Education (Fundamentals) services, namely:
    - Google Mail, Docs, Slides, Sheets, Chat, Calendar, Meet (replaces Zoom);
    - Google Drive (+ Gmail) with max storage of 50GB;
- my.Laurentian;
- Library access;
- Access to desktop security software (must adhere to the Laurentian IT computer standard; call or email the IT service desk);
- Adhere to Laurentian's Acceptable Use Policy and other IT policies; and,
- Service Desk support for the services listed above.

Engagement Obligations

Retired faculty who retain IT privileges are expected to comply with this Policy and other IT policies, and complete all mandatory Cyber-security training and other digital training as required (and communicated).