LaurentianUniversity
UniversitéLaurentienne

Policy on Managing Confidential Digital Information

Office of Administration:	Associate Vice-President, Information Technology
Approval Authority:	President and Executive Team
Approval Date:	April 23 2019
Last Review:	July 09, 2019
Next Review:	June 2022
Review History:	April 2015, April 2019

1. Purpose

1.1 In conjunction with the principles outlined in the Laurentian University Policy on Freedom of Information and Protection of Privacy, the purpose of the Laurentian University's Policy on Managing Confidential Digital Information ("the Policy") is to:

1.1.1 Protect the confidentiality, integrity and availability of digital confidential information; and

1.1.2 Stipulate, clarify and outline authorized digital storage and transmission method of data so as to effectively manage and mitigate the risk of unauthorized storage and transmission of confidential digital information in order to prevent any risks related with Laurentian University of Sudbury ("the University") and the *Freedom of Information and Protection of Privacy Act*.

2. Scope

2.1 The Policy applies to all administrators, faculty, staff, contractors, students employed by the University, and volunteers of the University and its affiliates, who, as part of their role and responsibilities, may store and transmit confidential information digitally.

2.2 Each individual who creates, uses, processes, stores, transfers, administers, and/or destroys confidential digital information is responsible and accountable for complying with this Policy.

2.3 Regardless of where the confidential digital information is stored, the University has legal and ethical obligations to ensure that the confidential digital information is managed in a manner that maximizes its utility while minimizing risk of unauthorized or inappropriate use or disclosure.

2.4 This Policy does not address the rights of individuals with respect to copyright or intellectual property.

3. Definitions

3.1 "Confidential Digital Information" is information about:

3.1.1 An identifiable individual, including:

3.1.1.1 biological identification such as information relating to the race, nationality or ethnic origin, colour, religion, age, sex, gender identification, sexual orientation or marital or family status of the individual, blood type, fingerprints, etc;

3.1.1.2 information relating to financial transactions in which the individual has been involved with the University such as credit card transactions, account balance;

3.1.1.3 information relating to the education or employment history of the individual;

3.1.1.4 information relating to the medical, psychiatric, psychological or criminal history of the individual;

3.1.1.5 any identifying number, symbol or other particular assigned to the individual, such as a student number or an employee number;

3.1.1.6 contact information such as address, telephone number, email address, personal electronic identity(ies) of the individual;

3.1.1.7 the personal opinions or views of the individual except if they relate to another individual;

3.1.1.8 correspondence sent to the University 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;

3.1.1.9 the views or opinions of another individual about the individual;

3.1.1.10 the individual's name if it appears with other private information relating to the individual or where disclosure of the name would reveal other private information about the individual;

3.1.2 Identifiable University records that are not deemed public and treated as confidential information; and

3.1.3 Government Confidential Identifications including:

3.1.3.1 Social Insurance Number, Social Security Number, Health Card, Driver's License and others.

3.2 "Record", "Data" and "Information" means any record of information however recorded or copied, whether in printed form, on film, by electronic means (digital and analog) or otherwise, and includes:

3.2.1 Correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a video, a machine-readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof; and

3.2.2 Any record or data that is capable of being produced from a machine-readable record under the control of the University by means of hardware and/or software or any other information storage equipment.

3.3 "Cloud Storage" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, that is digitally stored on a device, media or service including:

3.3.1 LU data centres;
3.3.2 Computer;
3.3.3 Removable storage device;
3.3.4 The cloud (the Internet);
3.3.5 Email;
3.3.6 Software; and
3.3.7 Any other electronic device that can store information.

3.4 "Computer Storage" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, that is digitally stored on a device, media or computer including:

3.4.1 Desktop computers and laptop;
3.4.2 Removable storage device; and,
3.4.3 Mobile device such as a cell phone.

3.5 "Permanent Storage" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, that is digitally stored more than five (5) days.

3.6 "Temporary Storage" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, that is digitally and consecutively stored for less than five (5) days.

3.7 "Transmission" and "Data Transmission" means the digital conveyance of information from one media to another, and may be referred as:

3.7.1 Sending;
3.7.2 Transferring;
3.7.3 Submitting;
3.7.4 Exchanging;
3.7.5 Uploading and downloading;
3.7.6 Sharing; and
3.7.7 Other descriptions that translates to transmission.

3.8 "Removable Storage" device is any type of storage device that can be removed from a computer or a mobile phone while the system is running, including:

3.8.1 USB stick, thumb drive and memory stick;

3.8.2 Floppy or magnetic storage such as tape;
3.8.3 Portable or removable hard drive;
3.8.4 Optical disk such as CD, DVD, Blu-Ray; and
3.8.5 Other removable storage devices.

3.9 "LU Credentials" refers to your Laurentian University username and password, managed by the University and the Password Policy.

3.10 LU approved services are applications that are managed or sanctioned by the University; LU approved services typically require LU credentials that follow the Password Policy. They include but are not limited to:
3.10.1 myLaurentian, LUNET, SecureFS and other Laurentian web portals;
3.10.2 D2L;
3.10.3 Google G Suite managed by LU (requires the LU ID credentials), which includes Laurentian managed Gmail, Google Doc, Google Sheets, and all other G Suite applications managed by Laurentian;
3.10.4 Colleague, WebAdvisor, Self Service (eg. Student Planning) and associated software (e.g. Synoptic, CROA/Business Objects, …);
3.10.5 SugarCRM, Fusion, Marketo;
3.10.6 Avaya, Avotus ICM, Zoom;
3.10.7 REDCap;
3.10.8 Orbis and other approved experiential learning platform(s); and,
3.10.9 Other LU approved services.

3.11 If a desired software or service is not listed in this Policy or on the IT intranet site, the software or service can be requested to the IT department (it@laurentian.ca). Each request will be seriously considered.

3.12 Unmanaged service and unmanaged Cloud service are services that are not administered, not sanctioned by IT and not listed in section 3.10. Such examples include:
3.12.1 Dropbox;
3.12.2 Google Drive and Google Docs (unless managed by LU);
3.12.3 Microsoft 365;
3.12.4 Apple iCloud;
3.12.5 Amazon Storage;
3.12.6 Web applications;
3.12.7 Mobile applications; and
3.12.8 Any other unsanctioned services.

4 Managing Confidential Digital Information

4.1 Storage

4.1.1 Confidential digital information must only be stored permanently onto services managed by Laurentian as described in section 3.10.

4.1.2 Confidential digital information must only be stored temporarily onto computer storage (as defined in Section 3.4) that are password protected and adhere to the University Policy on Passwords.

4.1.3 Confidential digital information cannot be stored permanently onto computer storage as defined in Section 3.4.

4.1.4 Confidential digital information cannot be stored, permanently or temporarily, onto unmanaged Cloud services.

4.2 Transmission

4.2.1 Transmission of confidential digital information is permitted within the university campus (wired and wireless networks).

4.2.1.1 Transmission of confidential digital information beyond the university campus is only permitted for applications and services deemed compliant with section 4.1, and, permitted over secure protocols using HTTPS (Secure HTTP) or over an approved virtual private network (VPN).

4.2.2 Transmission of confidential digital information is not permitted onto unmanaged Cloud services including social media sites.

4.2.3 Transmission of confidential digital information is not permitted via an unmanaged service such as a mobile messaging system (texting) except when the service utilizes secure and encrypted Laurentian managed services.

4.3 Anti-virus and Anti-malware.

4.3.1 All desktops and laptops purchased with LU funds must be equipped and active with IT approved anti-virus/anti-malware software as defined per type of device.

4.4 Sending Emails

4.4.1 Email addresses become confidential when a large list of recipients (more than 50) can be contextualized, such as emails associated to the University, or large list associated to an Academic Department, and so on.

4.4.1.1 An email destined to a large list of recipients of 100 or greater must be sent as a “Bcc:” (blind copy) instead of “To:”.

4.4.1.2 It is recommended that an email destined to a list larger than 50 and smaller than 100 should be sent as a “Bcc:”.

4.5 Disposal of Confidential Digital Information

4.5.1 All digital or analog devices that currently contain or contained confidential digital information must be securely disposed by IT (Information Technology Department); contact IT service desk for disposal.

4.5.2 Any approved Laurentian computer storage or devices that temporarily stored confidential digital information must be deleted (trash emptied) within five (5) days.

4.6 Software and services that will store Confidential Digital Information must be approved and must be administered by IT. Any deviation must be approved by the Associate Vice-President, (AVP) Information Technology.

5 Compliance

5.1 Disciplinary or other action may be necessary in instances where work practices or other activities are in contravention of, or not in accordance with, this Policy. In doing so, the rights and obligations established by collective agreements and university policy will be honoured.

5.2 Requested exceptions to the requirements as outlined in the Policy shall be made in writing, to the AVP, IT. The AVP IT may consult with the University Secretary and General Counsel.