Category:	**Technology and Information Management**
Approved By:	**College Leadership Council (CLC)**
Approval Date:	**April 17, 2018**
Effective Date:	**May 17, 2018**
Revised Date(s):	
Policy Sponsor:	**Vice President Corporate Services and Chief Financial Officer**
Policy Administrator:	**Director Information Technology Services**

Information Technology Security Policy

Purpose

The purpose of this policy is to protect the confidentiality, integrity and availability of Lethbridge College information technology resources from threats that include, but are not limited to, unauthorized intrusions, malicious use, and inadvertent compromise. Lethbridge College relies on information technology resources to conduct its business; the availability and integrity of information technology resources is essential to college operations.

Scope / Limits

This policy applies to all members of the college community who access Lethbridge College information technology resources.

Definitions

Information Technology Resource any Lethbridge College computer, device, network or room which creates, retrieves, manipulates, transmits or stores sensitive information. This includes, but is not limited to, central and non-centrally supported computers, file systems attached to these computers, operating systems running on these computers, software packages supported by these operating systems, wired and wireless networks, telecommunication and hand-held devices, data stored on or in transit on the above, as well as electronic identities used to identify and authenticate the users of information technology resources.

Information Technology Security Framework The program that ensures responsible controls, risk assessment and system scrutiny are in place to guarantee availability, integrity and confidentiality of Lethbridge College information technology systems and data.

Member(s) of the college community Includes board of governors members, employees, minors, parent/guardian, student, third party contractor, visitors, volunteers, and renters or persons booking college facilities, any individual directly connected to any college activity.

Policy Statements

1. The use of Lethbridge College information technology resources will comply with all applicable Federal and Provincial laws, as well as applicable industry regulations.

2. Lethbridge College will maintain an Information Technology Security Framework, which will be coordinated through the Information Technology Services (ITS) department.

3. Responsible use of Lethbridge College information technology resources will be governed by the Use of Information Technology Resources Policy and the accompanying procedures.

4. ITS will identify information technology security risks as prescribed in the Risk Management Policy and ensure that these risks are mitigated.

5. Any information system controlled by Lethbridge College, which stores, processes or transmits college data, will be secured in a manner that is considered reasonable and appropriate.

6. Throughout its lifecycle, all college data residing on information technology resources will be protected in a manner that is considered reasonable and appropriate.

7. Violations of this policy may result in suspension for a period of time or loss of the violator's use privileges with respect to Lethbridge College owned information technology systems and data. Additional administrative penalties may be applied up to and including termination of employment or contractor status with Lethbridge College. Civil, criminal and equitable solutions may be pursued. Students Rights and Code of Conduct Policy and procedures may apply along with provincial and federal legislation.

A: Policy Supports

Use of Information Technology Resources Procedures (Appendix A)

B: Legislated References

C: Other References

Alberta Post-secondary System ITM Control Framework Program
COBIT (Control Objectives for Information and Related Technologies)
ISO 27001 Specifications for an Information Security Management System
ITS Procedure 015 Security Standards

D: Related Policies

Confidentiality
Records Management
Respectful Campus
Risk Management

Social Media
Student Rights and Code of Conduct
Use of Information Technology Resources
Board of Governors:
EL-5 Asset Protection

Parent Policy:	**Information Technology Security**
Effective Date:	**May 1, 2019**
Revised Date(s):	**May 1, 2019, April 17, 2018**
Policy Sponsor:	**Vice President Corporate Services and Chief Financial Officer**
Policy Administrator:	**Director Information Technology Services**
Appendix A	

Use of Information Technology Resources Procedures

General Procedures

1. Information technology resources are to be used primarily for administrative and educational purposes (i.e. instruction, teaching, educational research and administration). All users have the responsibility to ensure that incidental personal use of college information technology resources does not interfere with the normal course of their duties.

2. Incidental personal use of information technology resources is permissible so long as the usage does not compromise or violate the network, computer, or data security and/or the ethical principles set forth by the college.

3. Individuals will not engage in unacceptable use of information technology resources, such as but not limited to the following:
   a. **Unauthorized access:** This may include using unauthorized user names, passwords, computer addresses or identities or modifying assigned network settings to gain access to computer resources and/or data, or otherwise attempting to evade, disable or exploit security provisions of college or external systems.
   b. **Unauthorized distribution and disclosure of records and information:** Every effort must be made to prevent the unauthorized disclosure and distribution of records and information that is under the custody and control of Lethbridge College.
   c. **Vandalism of data:** Deliberate alteration or destruction of computer files is a Criminal Code offence. Under no circumstance may a user inspect, alter, delete, publish or otherwise tamper with files or file structures that the individual is not authorized to access. The Alberta Freedom of Information and Protection of Privacy Act (FOIP) also deals with deliberate destruction of records.
   d. **Interference with other users' work:** This includes use of any process that causes a user to be deprived of services or resources that they would normally expect to have available. It covers but is not limited to the creation of "spam" (excessive email distribution), and the introduction of viruses or electronic chain letters.
   e. **Squandering resources:** Resources are shared and no user may degrade the systems by: unwarranted data space, time and bandwidth consumption through resource-intensive programs, unattended network connections and/or lengthy print jobs.
   f. **Sharing of account:** The college's information technology resources are allocated to groups and individuals for specific administrative and academic purposes. It is not acceptable to give, sell, or otherwise provide information technology resources to other individuals or groups that do not have explicit permission to use them. Users are not to

share computer accounts without obtaining permission from college administration and/or Information Technology Services (ITS).

g. **Commercial uses:** The college's information technology resources are allocated to groups and individuals for specific academic and administrative purposes and are not to be used for commercial purposes unless deemed a college sponsored initiative
h. **Breach of copyright:** This includes installing, reproducing and/or distributing copyrighted materials such as proprietary software, published materials or other works without permission. College software is provided under license agreements with various vendors and may not be copied or otherwise removed. Third party copyrighted materials that the users do not have specific approval to store and/or use, must not be stored on college systems or networks.
i. **Offensive material:** Other than activities approved for academic or scholarly purposes, materials not subject to legal sanction may be objectionable or extremely offensive to persons other than the information technology resource user. Importation or distribution of such material (including, but not limited to racist material, hate literature, sexist slurs or sexually explicit material) is permitted for academic or research purposes as long as it complies with applicable college policy. It is recommended that prior consultation with a Dean or Director be obtained to ensure that the college's ethical standards are maintained.
j. **Hostile atmosphere:** It is unacceptable to display sexually explicit or violent images in public spaces and/or to initiate unsolicited communication with sexual content.
k. **Harassment:** Harassing or defamatory material must not be sent by electronic means, including but not limited to, email, texting, voice mail, or posts to social groups such as Facebook, Twitter, etc. The Criminal Code of Canada outlines the offense and punishments.

4. Individuals will use information technology resources in a safe and secure manner. This includes but is not limited to the following:
   a. **Device protection:** Members of the college community using college-owned devices are responsible for the following:
      i. To maintain a backup of all important data stored on the device.
      ii. To take the necessary steps to protect the device from theft and/or misuse.
      iii. User installed software must be appropriately licensed and from a trusted source.
      iv. Individuals are prohibited from removing or disabling security software.
      v. Individuals are to return devices to the college when requested.
   b. **Mandatory training:** ITS will provide security awareness training for staff. Employees must participate in this training to ensure they are taking the necessary steps to protect the college's assets from cyber-threats.
   c. **Personal devices:** Members of the college community using personal devices are responsible for the following:
      i. Personal devices cannot be plugged into the college's wired network. Personal devices are to be connected to the appropriate wireless network.
      ii. Accessing college assets such as email or work files should be done via the applications cloud portal, for example Canvas or Office 365. This keeps the assets in a safe location and not locally stored on the personal device.
      iii. If it is necessary to download and store college assets on a personal device, then that device must be password protected and encrypted. To

protect personal, confidential and sensitive information stored on a personal device please refer to the Computer and Mobile device security section of the ITS website.

5. Users are expected to practice sound password management by respecting the following guidelines:
    a. Passwords must be created and solely maintained by the user without outside influence or assistance.
    b. Passwords must be a minimum of 12 characters in length.
    c. Passwords must contain at least three of the four following character types: (1) uppercase letter, (2) lowercase letter, (3) number, (4) ASCII special character (excluding periods, spaces, Unicode characters).
    d. Passwords must not contain common words, personal information, or simple keyboard patterns such as QWERTY. Passwords should be a sequence of characters that do not have a specific meaning to anyone other than the user who created it.
    e. An easy way to create a long secure password is to combine phrases with special characters.
    Eg. *This is smart* and *college rules* becomes Th1$_is $mart and C0lleg3-ru1es
    f. Passwords must be treated as confidential information and must be unique (ie: not re-used by the user on other platforms). When resetting passwords, users must create a new password which they have not used in the past at Lethbridge College.

6. The college will provide students with email and account services for 18 months after the last class a student is enrolled in. After this date, the account will be deleted.

7. As the use of college information technology resources and technology capabilities change over time, users should work with ITS in defining appropriate and efficient uses of information technology resources.

8. In the event of a security breach or an event which is causing a severe degradation in network performance, ITS will immediately act to stop the security breach or the event which is causing a severe degradation to the computing and networking environment in order to protect the environment.

9. ITS is available to assist, advise and consult with users on the acceptable use of college information technology resources and interpretation of this policy. Requests should be routed through the ITS Help Desk.
10. If the college learns of an unacceptable use of information technology resources, action will be taken as specified in the Reporting Procedures, Investigation Procedures, Employee Account Access Procedures and Disciplinary Procedures.

Reporting Procedures

1. If a member of the college community discovers inappropriate use of information technology resources, he/she should report the inappropriate use to his/her Dean or Director. Those not comfortable addressing the issue with a Dean or Director, or not satisfied with their response, may bring their concern forward to the Vice-President People

and Planning, the Director of ITS, or to any other Lethbridge College administrator, manager or director.

2. If, in the course of managing the computing and networking environment, an ITS employee discovers inappropriate use of the resources, he/she should report the inappropriate use to the Director of ITS.

3. All disclosures made under this policy and all investigations will be handled in a confidential and sensitive manner and will be only disclosed to parties that have a legitimate need to know, or as required by law.

Investigation Procedures

1. Suspected violations of this policy will be investigated in a fair and consistent manner and appropriate action taken. An investigation is a systematic process of scrutinizing the activities of an individual or group suspected of violation of this policy. An investigation will only proceed upon the written authorization (email is acceptable) from the President or a Vice President.

2. An investigation may include, but is not limited to, retrieving files and email, documenting Internet activities using monitoring tools, and analysis of system log files. An investigation does not include the routine monitoring of information technology resources by ITS to ensure adequate, secure and consistent delivery of these resources.

3. The objective of an investigation will be to establish, at least, any or all of the following:

    - provide assignment or responsibility for investigating the specific incident
    - determine whether the report of unacceptable use of information technology resources is substantiated
    - provide a professional response to any unacceptable use of information technology resources issue
    - assist in mitigating the effects of the situation
    - assist in recommending methods to reduce or eliminate the probability of similar types of occurrences
    - determine if disciplinary or legal action needs to be taken

4. Investigations regarding information technology resources will be coordinated by the Director of ITS. Under their direction, ITS staff will:

    - gather appropriate documentation of the information technology resources being used in an unacceptable manner by the individual or group
    - analyze the findings and generate a report
    - present the findings report to the Director of ITS who in turn will present the report to the appropriate Vice President for review and action

5. Investigations involving students will follow the Students Rights and Code of Conduct Policy and procedures.

6. When appropriate, investigations may be handled by outside authorities.

Employee Account Access Procedures

1. When an employee is no longer with the organization or there is a legal requirement, there may be a need for a supervisor or other designated college employee to access their email, files or phone messages in order to continue smooth operations within the college.

2. To access such information, the requestor must fill out the Employee Account Access Request Form and submit it to the Director, Information Technology Services. The form will be reviewed and if appropriate, approved by the Director, ITS and the Vice-President Corporate Services and Chief Financial Officer.

3. All employee account access requests are processed with the upmost seriousness. Providing access to an employee's account is not a given and will be scrutinized and questioned as necessary.

4. If full/partial access is granted, ITS staff will provide the requestor with the appropriate access for a finite amount of time

Accessing a student account would follow the same process as accessing an employee account.

Disciplinary Procedures

1. Substantiated cases of failure to follow this policy may be cause for the following actions:
    a. **Employees:** removal of access to Information Technology Resources at the discretion of the Director, Information Technology Services or delegate. More serious offences requiring disciplinary action will be referred to the Respectful Campus Policy and Procedure or provincial and federal legislation.
    b. **Students:** removal of access to Information Technology Resources at the discretion of the Director, Information Technology Services or delegate. The Students Rights and Code of Conduct Policy and procedures may apply along with provincial and federal legislation.
    c. **Third Party Consultants and Contract Staff:** possible termination with the college.

2. Allegations that prove not to be substantiated and made maliciously or knowingly to be false will be viewed as a serious disciplinary offense, and dealt with appropriately. Actions for staff may include discipline up to and including termination of employment or association with the college, and/or legal sanctions. Actions for students will follow Disciplinary Procedures 1.b). A complainant who has acted in accordance with the requirements of this policy and the related procedure is protected against reprisal.