IT 05 Information Sensitivity and Security

Classification:	Information Technology
Responsible Authority:	Director, Information, Institutional Research and Technology Services (IIRTS)
Executive Sponsor:	Vice President, Business Development
Approval Authority:	President's Executive Committee
Date First Approved:	2009-04-01
Date Last Reviewed:	2012-05-16
Mandatory Review Date:	2017-05-16

PURPOSE

This policy assists employees to determine the relative sensitivity of College information they can access and identify what information should not be disclosed without proper authorization. The information covered by this policy includes, but is not limited to, information that is either stored or shared via any means, including electronic information, information on paper, and information shared orally or visually by telephone or video conferencing.

SCOPE

This policy applies to all employees, students, contractors, vendors and volunteers of the College, and to all information systems and devices that connect to or access the College's wired or wireless networks.

DEFINITIONS

Word/Term	Definition
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording and destruction
Information Sensitivity	The control of access to information or knowledge that might result in loss of an advantage or level of security if disclosed to others who might have low or unknown trustability or undesirable intentions
College Community	All employees, students, contractors, vendors, and volunteers to the College

POLICY

1. Employees, students, contractors, vendors and volunteers of the College will take reasonable steps to protect the privacy, integrity, and availability of College information they access. The precautions required to protect College information are determined by the sensitivity of the information, and as required by legislation, including:
   - The Freedom of Information and Protection of Privacy Act, 1987, Province of Ontario (FIPPA);

- The Personal Information Protection and Electronic Documents Act, 2004, Government of Canada (PIPEDA); and
- The Patriot Act, 2002, Government of the United States of America.

2. Individuals will only be granted privileges and access rights to data held by the College, information systems and networks they require for their work, research, or education. When an individual's responsibilities change, their privileges and access rights are to be reviewed and adjusted accordingly.

3. Where information is presented in physical or digital format, a statement will indicate where the authoritative, current source of the information can be located.

4. Data of a sensitive nature will be identified as such by the author.

5. Data that is of a personal nature will, within the bounds of business conduct, be governed by a privacy policy that allows the user to opt out of having their data used for non-mandatory purposes.

6. **Classification of College Information**

6.1 All College information, regardless of where it resides or what purpose(s) it serves, will be consistently protected throughout its life cycle based on its sensitivity and its importance to College operations. All College information is categorized into three main classifications:

a. Public Information

This is information intended for public use that, when used as intended, will have no adverse effect on the operations, assets, or reputation of the College, or the College's obligations concerning information privacy. The College reserves the right to control the content and format of Public information.

Examples include program monographs, syllabi, business phone numbers of staff, and campus maps.

b. Internal Information

Internal information is intended for use by and made available to members of the College Community who have clearly identified a business need. If this information is disclosed, it will have minimal or no adverse effect on the operations, assets, or reputation of the College, or the College's obligations concerning information privacy. Internal information may be released to external parties to the extent there is a legitimate business need to do so. The College reserves the right to control the content and format of internal information when it is published to external parties.

Examples include internal memos, minutes of meetings, and internal project reports.

c. Sensitive Information

This is information intended for limited use and be made available only to authorized persons within the College. If disclosed, this information can be expected to have a serious adverse effect on the operations, assets, or reputation of the College, or the College's obligations concerning information privacy.

Examples include employee and student information, appeal and grievances, logical or physical architectures, accounting information, and information protected by legislation.

Documents, classified as sensitive information, are to be marked “confidential” and never left unattended or unsecured.

6.2 All employees and third parties who have access to sensitive information will be asked to sign a written acknowledgement of having read this policy, and agreeing to comply with its provisions.

7. **Security Regulations**

7.1 The College will employ various measures to protect the security of its computing resources and its users' accounts. Users will be responsible for the security and protection of the information resources over which they have control. Resources to be protected include networks, computers, software, portable storage devices (such as flash drives) and data. Further users are responsible for their use of external software including applications and storage that may compromise the security and management of the Colleges resources, accounts and information.

7.2 All online or web accessible Student Information will reside on secure College owned and operated servers or on approved external third party operated servers, and be readily accessible only to College employees responsible for the administration of such information.

7.3 The use of an external ASP other than the College owned and operated servers to house Algonquin student information must include an agreement with clear indications on security, privacy and backup procedures, signed by the Director, IIRTS, the Vice President, Administration and the Vice President, Academic .

7.4 Users of the College computing resources will engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly. Activities performed off-site must comply with the same security requirements as in-house activities.

7.5 ITS will ensure that login and password change routines for use of College directories employ current, industry standard secure methods for encryption of passwords.

7.6 All passwords at the College, regardless of what they secure, must adhere to the following rules:

a. Password lengths are at a minimum 8 characters;
b. Passwords make use of both upper- and lower-case letters (case sensitivity) and include one or more numerical digits;
c. Passwords are not words found in a dictionary or based on the user's personal information.
d. Passwords are to be changed at a minimum once every one hundred and twenty (120) days but will also allow users to change passwords more frequently if desired;
e. Passwords may not be reused within two years.

7.7 ITS will ensure that procedures are in place to reset a user password with authorization from the System Owner or designate.

7.8 The College will use secure sockets layer (SSL) to ensure that all financial transactions are safe, secure and in compliance with Payment Card Industry (PCI) mandates and policies.

7.9 From time to time, the College may monitor individual usage of its computing resources as part of the normal operation and maintenance of the College's computing resources. This includes the monitoring of usage of computing resources by users, the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service.

7.10 The College may also specifically monitor the activity and accounts of individual users of College computing resources, including individual sessions and communications, without notice, when:

a. The user has voluntarily made them accessible to the public, by posting to Usenet or a web page.
b. It appears necessary to do so to protect the integrity, security, or functionality of the College or other computing resources or to protect the College from liability.
c. There is reasonable cause to believe that the user has violated, or is violating, this or any other College policy.
d. An account appears to be engaged in excessive activity, as indicated by the monitoring of general activity and usage patterns.
e. It is otherwise required or permitted by law.

7.11 The College, at its discretion, may disclose the results of any general or individual monitoring, including the contents and records of individual communications, to appropriate College officials and/or municipal, provincial or federal law enforcement agencies and may use those results in appropriate College disciplinary proceedings or in litigation.

7.12 Users who engage in electronic communications with persons in other provinces or countries or on other systems or networks should be aware that they may also be subject to the laws of those other provinces and countries and the rules and policies of those other systems and networks including the privacy rights afforded the personal data of residents of those jurisdictions.

7.13 Users must ensure that the use of any downloaded material (including print, audio, and video) stored on College or a personal computer respects copyright laws.

8. PROHIBITED ACTIVITIES

8.1 This policy prohibits the following activities:

a. Interfering with, tampering with, or disrupting systems;
b. Intentionally transmitting any computer viruses, worms, key loggers or other malicious software;
c. Attempting to access, accessing, or exploiting resources not authorized by the individual user;
d. Knowingly enabling inappropriate levels of access or exploitation of resources by others;
e. Downloading sensitive or confidential information/data to computers that are not adequately configured to protect it from unauthorized access;
f. Disclosing any information/data the user does not have a right to disclose.

9. Enforcement

9.1 Any user found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment or expulsion from the College.

PROCEDURES

	ACTION	RESPONSIBILITY
1.	**Protection of College Sensitive Information**	
1.1	Provide training to all employees on their obligations regarding the protection of College sensitive information, and the procedures to protect non-public personal information from unauthorized access, improper use, or destruction.	IIRTS and Centre for Organizational Learning
1.2	Request all employees and third parties who are granted access privileges to sign a written acknowledgement of having read this policy, and agreeing to comply with its provisions.	Immediate supervisor
1.3	Encrypt all data containing non-public personal information and other sensitive information before it is electronically transmitted.	End users
2.	**Secure and Proprietary Information**	
2.1	Change system level and user level passwords at least every one hundred and twenty (120) days.	End users
2.2	Ensure all computers, laptops and workstations are secured with a password-protected screensaver with the automatic activation feature set at thirty (30) minutes or less, or by logging-off (Ctrl+Alt+Del for Windows 2000 or later users) when the work station host will be unattended.	ITS Staff
2.3	Teach all staff or third parties to ensure that sensitive information is not stored on any portable computer or portable electronic device unless the information is encrypted in accordance with this policy.	ITS Staff
2.4	Protect all equipment from viruses and other malicious software connected to the College network, whether owned by the authorized user or the College, by using approved virus-scanning software with a current virus database.	End users
2.5	Teach authorized users to recognize potential hazards when opening e-mail attachments, which could contain viruses, e-mail bombs, or Trojan horse code.	ITS Staff
3.	**Remote Access**	
3.1	Submit the request to use an external ASP to house sensitive information, including Algonquin student information, to their immediate supervisor who, in turn, will forward the request for approval to the appropriate Vice President and the	Employee wanting to use external ASP

	Director, IIRTS.	
3.2	If the request is approved by the Vice President and the Director, IIRTS, obtain an agreement with indications on security, privacy and backup procedures, signed by a Senior Administrator of the ASP, the Vice President and the Director, IIRTS.	Employee and ITS staff
3.3	Ensure that access to sensitive information housed outside the College's network is made available only to those employees or third party vendors with a demonstrable need for access to that information.	Immediate supervisor and Information Security Officer
4.	**Computer-to-Analog Line Connections**	
4.1	Grant written waivers to the policy prohibiting Computer-to-Analog Line Connections on a case by case basis for a limited time period.	Director, IIRTS
5.	**Database Storing Sensitive Information**	
5.1	Maintain the security of sensitive information on an internally stored database, granting access by software programs after authentication with credentials.	Director, IIRTS or Information Security Officer
6.	**Database User Names and Passwords**	
6.1	Store database user names and passwords in a file separate from the executing body of the program's code. This file shall only be accessible by authorized users.	ITS Staff
6.2	Ensure that database user names and passwords are read from the file immediately prior to use if stored in a file that is not source code, and that immediately following database authentication, the memory containing the user name and password is released or cleared.	ITS Staff
7.	**Password Procedures**	
7.1	For all servers, network attached devices and infrastructure management devices including switches, firewalls, routers and other technology, select and maintain passwords in accordance with the guidelines below: a. All system-level passwords (e.g., root, enable, administration, application administration accounts, etc.) must be changed at least 120 days; b. All user-level passwords (e.g., email, web, network, etc.) must be changed at least every 120 days; c. Passwords are not to be reused for two years; d. Passwords are not be transmitted in any form of non-encrypted electronic communication. e. Where Simple Network Management Protocol (SNMP) is used, the community strings should be defined as	ITS Staff and end users

	something other than the standard defaults of "public," "private" and "system" and should be different from the passwords used to log in interactively. A keyed hash should be used where available (e.g., SNMPv2). f. All user-level and system-level passwords should conform to the guidelines described in 7.2 below.	
7.2	For all end user devices, including desktop and laptop computers and College supplied smartphones, tablets and other devices, select and maintain passwords based on the following guidelines: a. Be at least 8 characters in length; b. Contain at least 3 of the 4 following password complexity requirements: i. Lowercase letters (e.g., a – z); ii. Uppercase letters (e.g., A – Z); iii. Numbers (e.g., 1 – 9); iv. Characters (e.g., (!@#$%^&*). c. Not found in a dictionary or based on personal information: names of family, pets, etc. d. Not written down or stored on-line.	End users
7.3	Control, either by a one-time password authentication or a public/private key system with a strong passphrase, the use of passwords for remote access users via insecure remote access methods such as computer-to-analog line connections,	ITS Staff
8.	**Anti-Virus Procedures**	
8.1	Request all authorized users to use anti-virus procedures for all computers and electronic devices connected to Algonquin College networks.	ITS Staff
9.	**Server Security**	
9.1	Establish and maintain approved server configuration and security guides.	ITS Staff
9.2	Monitor configuration and security compliance of the servers, including an exception policy tailored to the College's environment.	ITS Staff
9.3	Maintain and routinely review logs and audit trails on: a. all security-related events on a weekly basis at a minimum b. higher security infrastructure and technology on a daily basis or automated to be more frequent.	Information Security Officer
10.	**Router Security Procedures**	
10.1	Maintain a required minimal security configuration procedure for all routers and switches connecting to a production network or used in a production capacity by the College.	ITS Staff

11.	**Wireless Communications Procedures**	
11.1	Maintain a procedure to prohibit access to the College networks via unsecured wireless communication mechanisms, which covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Algonquin College's internal networks, including any form of wireless communication device capable of transmitting packet data.	ITS Staff

SUPPORTING DOCUMENTATION

None

RELATED POLICIES

AA 34 Copyright
AA 35 Confidentiality of Student Information
AD 02 Freedom of Information and Protection of Privacy

RELATED MATERIALS

Office of the Information and Privacy Commission of Ontario. *Procedures Manual*
http://www.ipc.on.ca/english/Resources/IPC-Corporate/IPC-Corporate-Summary/?id=665