

ALGONQUIN COLLEGE DIRECTIVE	NO. OF PAGES 3	DIRECTIVE NO. A25
	ORIGINATOR College Technologies Committee	
	APPROVED BY President's Executive Committee	
TITLE College Information Security	EFFECTIVE DATE 2009.04.01 <small>(with full implementation by December 31, 2009)</small>	REPLACES New

PREAMBLE

In order to fulfill its mission of teaching, research and public service, the College is committed to providing a secure yet open network that protects the integrity and confidentiality of College information while maintaining its accessibility.

The physical and logical integrity of the Colleges networks, computers, software, and data resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise.

POLICY

Each member of the College community is responsible for the security and protection of information resources over which he or she has control. Resources to be protected include networks, computers, software, and data.

Users who are authorized to obtain or access data must ensure that it is protected to the extent required by law or College policy.

Activities performed off-site must comply with the same security requirements as in-house activities.

PROCEDURES, ROLES AND RESPONSIBILITIES

1. System owners and the College's Information Technology Services Department (ITS) are responsible for the review and approval of the means used to provide the security for confidential data. They are to determine a process to determine which authorized users may access such data and the level of access that will be permitted.

2. The primary business contact for each system (System Owners) and ITS must ensure an appropriate process is in place to monitor access to confidential information. Where possible, change records or audit trails are to be maintained for modification of confidential data
3. ITS will assist system owners to ensure that:
 - a. requests for authorization for access to confidential data and assignment of the level of access privilege is reviewed by the System Owner or designate.
 - b. authorization records are retained consistent with College records retention guidelines.
4. Individual users of College systems and networked resources will be required to:
 - a. change their network access and system access passwords according to the established schedule.
 - b. ensure passwords are not shared for access to data that is confidential.
5. ITS will ensure that login and password change routines that use the College directories use current, industry standard secure methods for encryption of passwords. Passwords at Algonquin College must all 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. Network systems will require passwords be changed at a minimum of once every 120 days but will also allow users to change passwords more frequently if desired.
 - e. Passwords may not be reused within 2 years.
6. ITS will ensure that procedures are in place to reset a user password with authorization from the System Owner or designate.

COMPLIANCE WITH LAW AND POLICY

In addition to any possible legal sanctions, violators of this Directive may be subject to disciplinary action up to and including dismissal or expulsion, pursuant

to College policies, collective bargaining agreements, codes of conduct, or other instrument governing the individual's relationship with the College. Recourse to such actions shall be as provided for under the provisions of those instruments.

PROHIBITED ACTIVITIES

The following activities are specifically prohibited under this Directive.

1. Interfering with, tampering with, or disrupting systems.
2. Intentionally transmitting any computer viruses, worms, key loggers or other malicious software.
3. Attempting to access, accessing, or exploiting resources you are not authorized to access.
4. Knowingly enabling inappropriate levels of access or exploitation of resources by others.
5. Downloading sensitive or confidential information/data to computers that are not adequately configured to protect it from unauthorized access.
6. Disclosing any information/data you do not have a right to disclose.

RELATED DIRECTIVES

A16 – Acceptable Use of Algonquin Networks and Accounts

E19 -Confidentiality of Student Records

E46 - Protection of and Access to Student Information and Course Material

Vice President, Administration