Confederation COLLEGE COLLEGE PRACTICE	Number: 7-2-01	# of Pages: 3
	Originator:	Computer Services
	Approved By:	College Planning Committee
	Replaces:	New
	Effective Date:	October 28, 2009

AUTHORIZED ACCESS TO INFORMATION TECHNOLOGY RESOURCES

Purpose

The computing and information technology resources of Confederation College support students and employees to support teaching, research, administrative, and learning activity. Access to computing and information technology resources is a privilege and the requirements for authorized access are outlined below.

Users who misuse the College's information technology resources are subject to the disciplinary actions specified in the Non-Compliance, Disciplinary Actions, and Appeals operating practice (7-2-03).

1 Authorized Access

Access to Confederation College's IT resources is provided through network login accounts. All students, staff, and faculty are issued individual accounts. Attached to each account are appropriate security and permissions necessary for the individual to access the systems and data necessary in their role at the College.

The College may also provide IT services or resources to others with whom it does business (e.g., alumni, contractors, retirees, visitors, or board members). Such requests for account access must be made to the Computer Services department from a manager in a department or area in the College authorized to make such a request.

Group or shared accounts are permitted only in exceptional circumstances. Special arrangements must be made with Computer Services in such instances. Responsibility for the shared account will be assigned to an individual.

Any person without an authorized College account is prohibited from using any and all College IT resources.

2 Unauthorized Access

Unauthorized access can include, but is not limited to, the following types of actions:

- using unauthorized accounts, computer addresses or identities,
- modifying assigned network settings/accounts to gain access to IT resources or information,
- otherwise attempting to evade, disable, or hack security provisions of the College or other external systems.

Persons using any information technology facilities for which they are not authorized may be committing an offence under the Criminal Code of Canada.

3 User Responsibilities

All College IT Resource users must:

- Upon request by College Security or Computer Services staff, be able to produce a valid College Student or Staff Photo ID card, or provide some other form of appropriate identification. Failure to so may result in the individual being escorted out of the computer lab or off the College's property.
- Comply with all College policies, rules, and regulations, as well as applicable federal and provincial laws.
- Comply with all definitions of acceptable and unacceptable use, as defined in the College's "Acceptable Use of Information Technology Resources" (7-1-01) policy.
- Use only those College computing resources that they are authorized to access and only for the purposes for which the access is granted.

4 Administrative Systems

Access to administrative College data is controlled through the access rights granted within the College ERP – SCT Banner. The system provides two web based interfaces to data with the system: 1) a self service module (SSB), and 2) a more detailed, fully functional interface (INB) intended primarily for more intense, comprehensive use of the system.

Regardless of the interface used to access Banner, individual rights are granted within four broad areas:

- Human Resource Module
- Finance Module
- Student Module
- General Access

All users of the College administrative system will have default access rights to data specific to their relationship with the College: In particular, using SSB:

- Employees have access to their payroll and other HR information.
- Budget holders have access to the details of their budgets and expenditures.
- Faculty have access to data for those students registered in the classes they teach.
- Students
- Everyone has access to their personal data (address, telephone, etc.)

In addition to default rights, Department managers can assign additional rights to INB users of Banner. These rights are primarily grouped in security classes – sets of INB functional screens that are required to complete related work at the College. Ex. Security class to create a position, create a purchase order, accept a student into a program, etc.

Individual access rights to Banner data are granted within three broad areas. These are listed below with the Banner module administrator – the College manager who has the responsibility of approving access rights to security classes within the module:

- Human Resource Module – Director of Human Resources
- Finance Module – Director of Finance
- Student Module – Director of Student Success/Registrar

Computer Services staff will implement data access changes only when authorized by the module administrator or their designate.

Managers must inform Computer Services whenever employee position changes result in changed access rights. Ex. Employee leaves the College, changes positions within a Department, etc.