JOHN ABBOTT
CEGEP/COLLEGE

# POLICY NO. 23

# Digital Information Security Policy

This policy was adopted for the first time by Resolution Number 386-09 to take effect on

June 1, 2018.

# Table of Contents

# *POLICY NO. 23 DIGITAL INFORMATION SECURITY POLICY*

## ARTICLE 1 - PREAMBLE

This policy allows John Abbott College (the “**College**”) to fulfill its mission, preserve its reputation, respect laws and reduce risks by protecting the digital information it creates, receives or holds in the course of its activities, whether it is kept by itself or by a third party (collectively, the “**Information**”). This Information can take on multiple and diverse electronic forms. It may consist of personal information of students and staff; professional information subject to intellectual property rights (teachers and researchers) and College strategic or operational information.

The digital world has no borders and is open to modern day pirates. These people, hidden in virtual space look for system vulnerabilities in order to successfully access and use various types of information to their benefit. Our College, as part of the higher education network, has a public image and is therefore a potential target.

In this context, the entry into force of the *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, G-1.03) (the “**LGGRI**”) and the *Directive sur la sécurité de l’information gouvernementale* (a Quebec Treasury Board directive applicable to CEGEPs) (the “**DSI**”) creates obligations for colleges in their capacity as public bodies. As such, the DSI requires colleges to adopt, implement, maintain and ensure the application of an Information security policy - the main terms of which are defined in the DSI – mainly by using formal information security processes to manage risk, access to information and incidents.

## ARTICLE 2 - OBJECTIVES

The objective of this policy is to affirm the commitment of the College to fulfill its obligations with regard to Information security. Specifically, the College must ensure that:

- Information is available in a way that it is accessible in a timely manner and only by authorized individuals;
- Information integrity is ensured so that it is neither destroyed nor altered in any way without proper authorization, and that the Information medium provides the necessary stability and longevity;
- Information remains confidential by limiting disclosure and ensuring use of the Information only by authorized persons, especially if it constitutes personal information.

As a result, the College is deploying this policy in order to guide and set its direction with regards to IT security matters. This policy strengthens internal control processes by providing reasonable assurance of compliance with government legislation and directives, as well as other risk reduction requirements associated with the protection of Information.

## ARTICLE 3 - LEGAL AND MANAGEMENT FRAMEWORK

This policy is framed by a context governed by, but not limited to:

- *Charte des droits et libertés de la personne* (LRQ, C-12);
- *Code civil du Québec* (LQ, 1991, 64);
- *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- *LGGRI*;
- *Loi concernant le cadre juridique des technologies de l'information* (LRQ, C-1.1);
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, A-2.1);
- *Loi sur les archives* (LRQ, A-21.1);
- *Code criminel* (LRC, 1985, C-46);
- *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (A-2.1, r. 2);
- *DSI*;
- *Loi sur le droit d'auteur* (LRC, 1985, C-42);
- *John Abbott College Policy No. 9 (Records Management and Archives)*;
- *John Abbott College Policy No. 20 (Risk Management Framework)*;
- *John Abbott College Policy No. 21 (Communications)*;

## ARTICLE 4 - SCOPE

This policy applies to all users of Information, that is, all natural or legal persons who, as employees, consultants, partners, suppliers, students or members of the general public, use College informational assets.

## ARTICLE 5 - GUIDING PRINCIPLES

The guiding principles for the College's actions in the area of Information security include:

a) Ensuring that the Information to be protected is well known by identifying those responsible for the Information as well as the characteristics of the Information that is to be secured. (It is, therefore, important to keep the inventory of informational assets up-to-date);

b) Relevant international standards are used to promote the deployment of best practices and to use comparative scales with similar bodies or institutions;

c) An acceptable risk-based approach is adhered to (allowing for evaluation of risk levels and for the implementation of a combination of reasonable measures to ensure Information security, at a cost proportionate to the sensitivity of the Information and the potential negative effects should the Information be compromised);

d) The importance of this policy is recognized and this policy is managed by a competent and appropriately sized team (this team must define, set up, operate and adjust the management of the security of the Information);

e) Personal information and other confidential Information is rigorously protected;

f) The technological environment is recognized as constantly changing and interconnected with the world. The security of the Information must be adaptable to changes in the technological environment;

g) The importance of regularly assessing risks, establishing proactive security measures and methods for detecting misuse or inappropriate use of Information, defining threat-eradication or recovery of compromised data methods must be recognized;

h) Information, throughout its lifecycle, from acquisition or creation to destruction must be protected. The level of security may vary over the lifecycle of the Information;

i) The principles of sharing best practices and operational information dealing with Information security with the education network and public bodies are to be favoured;

j) An ethical approach to ensure the regulation of conduct and individual accountability is imperative. Each individual who has access to Information is responsible for respecting the confidentiality, availability and integrity of the Information;

k) Each employee has access to the minimum Information required to perform his or her normal duties;

l) Transparent communication with respect to threats to informational assets is done in order to facilitate an understanding of the importance of applying the prescribed security measures and be informed so as to recognize security incidents and act accordingly;

m) A business continuity plan that allows the restoration of essential services to its clientele in a timely manner is to be established.

## ARTICLE 6 - MANAGEMENT FRAMEWORK

The effectiveness of Information security measures requires the clear allocation of roles and responsibilities to the various College stakeholders through the establishment of this policy which allows for adequate accountability.

Information security practices and solutions should be reviewed periodically to reflect not only legal, organizational, technological, physical and environmental changes, but also the evolution of threats, risks and vulnerabilities.

This policy is based on three fundamental management areas. These are access management, risk management and incident management.

## 6.1 Access Management

Access to various systems must be managed and controlled to ensure that access to, disclosure of and use of Information is strictly reserved to authorized persons. These measures are taken to protect the integrity and confidentiality of personal data and information.

The effectiveness of Information security measures rests on the assignment of responsibilities and accountability of all levels of the College staff. In such respect, see Appendix A which shall form an integral part of this policy.

## 6.2 Risk Management

A categorization of “up-to-date informational assets” supports risk analysis by providing knowledge on the value of the Information to be protected.

Risk analysis also guides the acquisition, development and operation of information systems, specifying the security measures to be implemented for their deployment in the College environment. The management of Information security risks is part of the College's overall risk management process. Government-wide risks are reported in accordance with the DSI.

The level of protection of Information is established on the basis of:

- the nature of the Information and its significance;
- probability of an incident, error or malevolence to which it may be exposed;
- the consequences of the materialization of these risks;
- the level of risk acceptable to the College.

## 6.3 Incident Management

The College deploys Information security measures in order to ensure the continuity of its services. In this regard, it shall put in place the necessary measures to achieve the following objectives:

- Limit the probability of occurrence of Information security incidents;
- Adequately manage these incidents to minimize the consequences and, where necessary, restore operations.

Information security incidents of government-wide proportion are to be reported in accordance with the DSI (to the CERT/AQ).

In the management of incidents, the College may exercise its powers and prerogatives with respect to any improper use of the Information it holds or of its information systems.

# ARTICLE 7 - ROLES AND RESPONSIBILITIES

This policy assigns the management of the College Information security to bodies, committees and individuals based on the particular duties they perform.

## 7.1 Board of Governors

The Board of Governors adopts this policy and any amendments thereto. The Board is regularly informed of the College's actions in the area of Information security. It is the head of the organization responsible for the application of this policy.

The executive committee and/or any other committee of the Board of Governors may take decisions within a framework previously determined by the Board of Governors.

## 7.2 Directors' Table

The Directors Table shall determine measures to promote the implementation of this policy and the College's legal obligations with respect to Information security. Thus, it determines the strategic orientations, the action plans and the risk assessment of College Information. It may also determine guidelines and procedures that clarify or support the application of this policy.

## 7.3 Information Security Working Group

The purpose of the Information Security Working Group is to assist the *Responsable de la Sécurité de l'Information* ("**RSI**") with this policy and other elements that may be required to ensure that the College is protected and complies with applicable regulations. It is a tactical and operational working group that meets as required.

This committee is responsible in particular for action plans and Information security reviews, awareness-raising or training activities and any proposals for action on Information security. It is also a forum for exchanges between stakeholders or observing the evolution of the Information security project.

The committee will be made up of key stakeholders of the College who will be directly involved in the security of Information.

This committee will be composed of the following persons: RSI, Director of ITS, key data owners (Director of HRS, Director of Finance, Registrar), CSGI, Manager of ITS Operations and Security, Security specialist (if applicable) and Manager of ITS Infrastructure.

## 7.4 Director General

The Director General shall ensure the application of this policy.

The Director General is responsible for:

- overseeing the RSI in carrying out its mandate;
- delegating certain Information management responsibilities to the Secretary General;
- having the Board adopt strategic directions, risk assessments, action plans, safety assessments, Information security accountability;
- authorizing (on an exceptional basis) a derogation from any of the provisions of this policy, a directive or an institutional procedure having a direct or indirect impact on the security of Information and which would be incompatible with an activity or project directly related to the mission of the College;
- authorizing an investigation where there is, or may be, a breach of this policy;
- maintaining a register of exemptions and a register of cases of violation of this policy.

## 7.5 Responsable de la sécurité de l’information (RSI)

The function of the RSI is delegated to a senior officer by the Board of Governors. In the case of the College, this is the Director of ITS. The RSI reports to the Director General as defined in the *Cadre gouvernemental de gestion de la sécurité de l’information*. This person ensures that the level of maturity in Information security management practices meets the College’s needs. This person is appointed by the Board of Governors.

The RSI :

- develops and proposes the College's information security program and reports its implementation to the Directors’ Table;
- makes recommendations with respect to the needs, priorities, directions, action plans, guidelines, procedures, initiatives and good practices in Information security and recommends appropriate updates to this policy;
- ensures the coordination and consistency of the College's actions in the area of Information security by advising the informational asset owners in the organization;
- produces the College's action plans, reports and accounts related to Information security;
- proposes provisions for compliance with Information security requirements to be incorporated into service agreements and contracts;
- ensures that the College reports any government-related Information security risks and incidents (CERT/AQ);
- collaborates in the development of the content of the communication plan, the information security training and awareness program and ensures their deployment;
- conducts investigations into serious transgressions pertaining specifically to this policy following the authorization by the Director General;

- ensures regulatory, legal, governmental and technological monitoring of changes in standards, laws and regulations, government practices and technological advances in Information security.

## 7.6 Coordonnateur Sectoriel de la Gestion des Incidents ("CSGI")

The CSGI collaborates closely with the *Ministère d'éducation et l'enseignement supérieur (MEES)* network's *coordonnateur organisationnel de gestion des incidents* ("**COGI-Network**"). The person in this role acts tactically and operationally to provide support with respect to incident management and risk management in IT. The CSGI is the official interface with the Computer Emergency Response Team de *l'Administration québecoise* ("**CERT/AQ**").

The CSGI in particular

1. Collaborates with the college network, COGI-Network and the RSI of their organization in the development of the various strategic and tactical elements in IT such as:
   - An IT policy;
   - A management framework;
   - A register of authority;
   - Categorization of assets;
   - Security measures for critical assets;
   - A formal risk management process in Information security;
   - A formal process for managing access rights to Information.

2. Participates actively in the COGI-Network implementation of the network of alerts in IT and establishes links with the other CSGIs in order to favour the sharing of expertise and tactical and operational elements to be developed and implemented;

3. Participates with the COGI-Network in the government incident management process, and in the government alert network coordinated by the CERT/AQ;

4. Develops and implements, with the support of the COGI-Network, a formal incident management and reporting process for their organization including an incident log from their organization;

5. Coordinates the management of IT Security incidents of their organization with governmental impact with the support of the COGI-Network:
   - Establishes, if it does not exist, an Incident Response Team ("**IRT**") in their organization;
   - With the members of the IRT, develops, implements and tests a response plan to security incidents of their organization;

6. Implements the appropriate response strategies for the College at the time of an incident, in conjunction with the COGI-Network.

## 7.7 Information Technology Services (“ITS”)

In the area of Information security, the ITS department ensures that Information security requirements are met throughout the information systems as well as in the execution of development projects or acquisition of new information systems in which they are involved; in such respect, the ITS department:

- is actively involved in risk analysis, assessment of needs and measures to be implemented, and anticipation of any security threats to information systems using information technology;
- applies appropriate response measures to any Information security threat or incident, such as interruption or temporary revocation - where circumstances require - of the services of an Information system using information technology to ensure the security of the Information in question;
- participates in the investigations relating to actual or apparent violations of this policy once authorized by the Director General.

## 7.8 Facilities Management Services (“FMS”)

The FMS department, together with the RSI, are involved in the identification of physical security measures to adequately protect the informational assets of the College.

## 7.9 Human Resources Services (“HRS”)

In terms of Information security, the HRS department obtains a commitment from all new College employees to comply with this policy.

## 7.10 Informational Assets Owner (“IAO”)

The IAO is the managerial authority within a department, whether pedagogical or administrative, whose role it is to authorize accessibility, use and security of informational assets under the responsibility of that service. There may therefore be several IAO in the College. The IAO may delegate all or part of their responsibility to another member of the service.

The IAO is responsible for:

- Informing the staff under its authority as well as third parties with whom the service collaborates of the provisions of this policy making them aware of the need to comply with it;
- Actively collaborating in the categorization of Information of the department under its responsibility and in the analysis of risks;
- Seeing to the protection of Information and information systems under its responsibility and ensuring that these are used by personnel under its authority in accordance with this policy;
- Ensuring that Information security requirements are taken into account in any acquisition process and any service contract under its responsibility and ensures that any consultant,

supplier, partner, guest, organization or external firm commit to this policy;

- Reporting any Information security threats or incidents to the ITS department;
- Collaborating in the implementation of any measure to improve the security of Information or to remedy an Information security incident as well as any Information security verification operation;
- Reporting to the Director General any problem associated with the application of this policy, including any actual or apparent violation of a staff member's application of this policy.

### 7.11 Users

The responsibility for the security of the College Information rests with all users of the College.

Any user who accesses, consults or deals with Information is responsible for its use and must proceed in such a way as to protect this Information.

To this end, the user must:

- comply with this policy and any other directive of the College on Information security and its use;
- use the access rights granted and authorized, Information and systems that are made available solely in the course of their duties and for the purposes for which they are intended;
- participate in the categorization of Information of their department;
- respect the security measures in place, not circumventing them, nor changing their configuration or disabling them;
- inform the IAO of any incident likely to constitute a violation of this policy or to constitute a threat to the security of College Information;
- collaborate in any intervention to identify a threat to Information security or an Information security incident;

All College users must therefore comply with the policies and directives in force in the course of their professional or academic activities when sharing informational assets, information technology or information systems.

## ARTICLE 8 - AWARENESS AND INFORMATION

Information security relies on the regulation of conduct and individual accountability. In this regard, members of the College community must be aware of:

- the security measures/program/policy applicable to College Information and its systems;
- the consequences of a breach of security;

- their role and responsibilities in this area.

To this end, awareness and training activities are to be offered periodically. In addition, explanatory documents are to be available on the College's system for information dissemination.

## ARTICLE 9 - SANCTIONS

In case of violation of this policy, the user engages their personal liability; the same shall apply to a person who, through negligence or omission, causes a situation that renders the Information inadequately protected.

Any member of the College community who contravenes the legal framework of this policy and its related Information security measures, is subject to sanctions depending on the nature, severity and consequences of the violation, in accordance with applicable laws or internal disciplinary rules.

Similarly, any violation of this policy, whether perpetrated by a supplier, partner, guest, consultant or external body, is punishable by the penalties provided for in the contract binding it to the College or under the provisions of the applicable legislation.

## ARTICLE 10 - DISSEMINATION AND UPDATING OF THIS POLICY

The RSI, assisted by the Directors' Table, is responsible for disseminating and updating this policy. This policy will be reviewed no later than three (3) years after its adoption.

## ARTICLE 11 - COMING INTO FORCE

This policy will come into force when enacted.

# Appendix A

## User Accounts

### Goal

The goal of this appendix is to lay out general principles and functioning rules for the management of user accounts and system access in order to permit the use of John Abbott College (the "**College**") resources including but not limited to the following services:

- E-mail,
- Server file and folder system,
- Locally stored data and
- Any system that contains personal and private information.

### Scope of this Appendix

This appendix applies to all personnel who need access to systems mentioned in the previous paragraph. In addition, this appendix also applies to external suppliers, contractors, agencies, etc. who have a contract with the College for maintenance purposes of Information Technology software and hardware, equipment or for any other purpose.

### Guiding Principles

The foundation for this document lies in the following directives:

The College[1]

- Grants only essential access rights to execute work-related tasks.
- Parameterizes passwords to reflect best practices in security guidelines[2].
- Never allows systems to display passwords.
- Blocks access to systems for ten (10) minutes after three (3) unsuccessful login attempts.
- Attributes temporary passwords when giving initial access to systems.
- Monitors use of all user accounts from which the internet is accessed.
- Locks screens after 15 minutes of non-use requiring the user to re-enter their password prior to logging back in.

The user has the obligation to:

- Change their password upon first accessing a system.

[1] Whenever the system allows or has the functionality built-in.

[2] Minimum of eight characters, contains 3 of 4 following groups: lowercase characters, uppercase characters, numbers, and special characters.

- Log on to JAC-Servers and save work-related documents on the College network[3] or Office 365 (i.e. One Drive) for safekeeping, and backup.
- Use the personal and confidential information that resides on our systems for the sole purpose of College work for which the data is intended or collected.
- Lock their workstation (Windows Key + L)[4] when not in use if it is accessible or in a public area.
- Use only their own account and password when logged on to computers.
- Follow the directives of this document as well as the Guidelines on Appropriate Usage of Computing Resources Including the Internet.

## Roles and Responsibilities

### The Information Technology Services (ITS) Department Management

The responsibility of the ITS department management is to:

- Manage network and email accounts.
- Manage access to all other accounts including those that had been historically decentralized[5]. This is with the exception of a new system currently in its testing or preliminary implementation phase.[6]
- Monitor and audit all College accounts.
- Monitor and audit all Internet traffic.
- Generate system access reports for the Informational Assets Owner (the "**IAO**")[7].
- Validate employee status with the data owner for the respective system.
- Revise this appendix regularly.

### The ITS Technicians

Under the direction of a Manager of ITS and/or the Director of Facilities Management and Information Technology Services, the general activities of the ITS technicians are to:

- Create, deactivate, reactivate, or delete "user" network, and email accounts, as requested by the respective Manager, Director of Facilities and ITS or from the Human Resources Services department.
- Assign rights to standard server folders as well as specific folders requested (via Octopus) by the immediate supervisor as applicable to their job function and approved by the data owner.

[3] Caution: ITS will not be able to assist you if documents are saved on "c" drive or other portable device in the case of a disaster or accidental mishap.

[4] The equivalent for Mac OSX is Control + Shift + Eject or Control + Shift + Power.

[5] Clara Finance, Clara Pedagogy and GEREMI are examples of decentralized systems. For these systems, the Dean/Director responsible for the system gives authorization for the staff member to have access. ITS department management grants access as authorized by the data owner.

[6] During this time, the Subject Matter Expert (SME) as designated by the responsible Dean/Director will assume this responsibility. Once the system moves into an "operation" phase, the ITS department will take on this responsibility and will validate all current and future access rights with the responsible Dean/Director. Any access deemed unnecessary/not pertinent to the job function of the user will be removed by the ITS department upon approval by the data owner.

[7] See Appendix B for table of IAOs.

- Advise the employee and the immediate supervisor of access to accounts when granted.
- Validate and adjust (with ITS management approval) access rights every 6 months as necessary.

### The Immediate Supervisors (Managers and Chairpersons)

Managers have the responsibility to ensure that their personnel are aware of this appendix. Users do not have the right to self-assign authorizations to systems.

Furthermore, immediate supervisors are to use the John Abbott College Service Centre (Octopus) for:

- Requests to create, reactivate, deactivate, or delete access codes for their personnel/colleagues.
- Requests to modify account settings (deactivate accounts, change passwords, or other temporary measures) for sick leaves, maternity/paternity, or other temporary leaves.
- The authorisation of granting access rights to departmental network folders when required (including re-activations after return to work).
- Giving authorization for access to their departmental systems (Clara Finance, Clara Pedagogy, Geremi, Octopus, etc.) under their responsibility for which they receive a request.
- Managing user names for departmental systems under their responsibility (Clara Finance, Clara Pedagogy, Geremi, Octopus, etc.).
- Requesting authorisation when a member of their staff needs access to a departmental system under their responsibility.

### The Human Resources Services (HRS) Department

- The Human Resources Services department will notify ITS and other required departments via e-mail, when an employee is newly hired (i.e. has signed their contract), changes department, is on extended leave, or is no longer employed by the College.

### The IAO

- The IAO authorizes or rejects accessibility to systems and data of informational assets under the responsibility of that service.
- The IAO regularly reviews the access reports generated by the ITS Department Management.

## Using College Accounts

### Administrator Rights

Administrator rights are not generally given to users for their computer. Administrator rights, when they are granted, are temporary and must be justified by nature of work and vetted by their Program Dean and

Academic Dean (faculty) or Director (support staff and professionals) and the Manager/Director of ITS. Once the nature of the work ends, the administrator rights are removed from the user.

It should be noted that in the case of issues with the functioning of a computer on which administrator rights have been granted to the user, no effort will be spent on the part of the ITS department to recover any data on this computer. The hard drive will be reformatted resulting in a loss of all data saved only on the computer's hard drive.

## Inside the College

Users have use of their workstation only for College work related activities.

## Outside the College

### Remote Access via Office 365

Users have access to their email account, calendar, and other services (One Drive, Share Point, MS-Office on line, etc.) through the Office 365 service.

### Remote Access via the Portal

Other services such as Omnivox, MIO, etc. are done through the College Portal (My JAC Portal). To access these services, the user must have an Active Directory account created as soon as a new employee signs their contract.

Users can access the following through the Portal @ https://johnabbott.omnivox.ca:

- Email account, and MIO mail box
- Limited server files by virtue of the My Files service
- Phone box configuration and phone messages
- LEA Classroom module
- Other Omnivox modules including their pay stubs, tax receipts, etc.

### Remote Access through a VPN (Virtual Private Network)

VPN access is a secure method to allow remote users to access the same files as they have available at work when away from the College environment. This access mode has a broad security issue since ITS cannot fully control the workstation that connects to the College network; therefore users must ensure that their computer has an active antivirus program installed and updated regularly. Access may be denied to any computer that does not have an active and updated antivirus program. We grant this mode for special cases only (i.e., administrators, IT technicians, and other authorized users.)

## Employment

### Newly Hired Employees

a. Once hired, the HRS department Director or delegate authorizes the creation of the employee account by email through Geremi (automatic mailing) to the ITS Department management with the following information:

   i. Employee name
   ii. Employee number
   iii. Employee department

b. Once hired, the HRS department also makes sure that the employee receives the link to the ITS "How-to" SharePoint site which gives information regarding the following and more:

   i. Computer Account
   ii. Office 365
   iii. My JAC Portal
   iv. Octopus
   v. Other items that can be requested through the Service Centre Software (Octopus) if and as required

      ITS related

      1. Phone line,
      2. CLARA Pedagogy (data owner approval required),
      3. CLARA Finance (data owner approval required),
      4. Computer (if none available),
      5. File folder access (data owner approval required),

      FMS related

      6. Keys (dean/director approval required),
      7. Furniture (if required).

c. ITS creates College accounts as per the information given in the "new employee" email:

   i. Active Directory Account
   ii. Phone Directory Entry

- For temporary employees, an end date must be present for the process to be completed.
- The ITS department may contact the immediate supervisor, director or dean to assure that all the information and rights are relevant.

- The ITS department transmits the Access Codes and temporary passwords directly to the new employee who in turn has the responsibility to change their password at first login.

### End of Employment (resigned, retired, or other)

When an employee leaves the College, either voluntarily or not, the immediate supervisor has the responsibility to inform the HRS department and then the HRS department must inform the ITS department of the last day of employment a minimum of 1 week in advance. Upon the departure date, the ITS department will temporarily archive[8] the contents of the personnel folder and set a redirection message on the employee's phone to another number as selected by the immediate supervisor. Note that, generally, voice mail boxes will not be maintained following last day of employment.

Therefore, prior to the end date, the immediate supervisor must assure that:

- All files relevant to the department or service (documents, letters, spreadsheets, databases, etc.) remain in the personnel's folder until ITS receives instructions from the employee's supervisor.
- The same is done for the employee's e-mail box.
- Retirees will have access to their e-mail box for as long as necessary provided there is on-going activity in the account and it is financially feasible for the College to maintain.
- The phone extension to which the departing employee's incoming calls should be redirected is determined. (This will occur for a period of one month after which the forwarding of calls will be terminated).

### Interdepartmental Transfers

When an employee transfers from one department to another, HRS has the responsibility to inform the ITS department of the last day of employment in the outgoing department as well as the first day of employment in the new department a minimum of 1 week in advance. (For temporary employees, an end date must be specified for the process to be completed.) The ITS department will take care of removing old accesses and granting new ones where necessary.

Therefore, once the transfer to the new department is approved, the HRS department Director or delegate authorizes the modification of the employee account accordingly by email to the ITS Department management. ITS will send a message to the employee's supervisor/chairperson to inform them of the new employee so that they can now request other items using the Service Centre Software (Octopus) if and as required:

i. Phone line (if required)
ii. CLARA pedagogy (if required),
iii. CLARA finance (if required),
iv. Computer (if none available),
v. Files folder access,
vi. Keys (if required),

[8] User files are archived at the time of departure in case something is missed and needs to be recovered. Full deletion of all past data is done in accordance with the College's data retention policies.

vii. Furniture (if required).

Prior to the end date, the outgoing immediate supervisor must assure that:

- All files relevant to the department or service (documents, letters, spreadsheets, databases, etc.) are transferred from the personnel folder of the employee to a departmental share folder.
- The same is done for the employee's e-mail box.

It should be noted that:

- The ITS department may contact the incoming immediate supervisor, director or dean to assure that all the information and rights are relevant.
- The ITS department transmits the Access Codes and temporary passwords directly to the new employee who in turn has the responsibility to change their password at first login.

# Appendix B

| System | Informational Assets Owner (IAO) |
|---|---|
| Pedagogical | Dean of Academic Systems |
| Financial | Director of Finance |
| HR Systems | Director of Human Resource Services |
| Residence | Director of Student Services |
| Casgrain | Director of Student Services |
| Departmental Folders | Director or Dean of the department |