ALGONQUIN COLLEGE

IT01 INFORMATION SECURITY

Classification:	Information Technology
Responsible Authority:	Chief Digital Officer, Information Technology Services (ITS)
Executive Sponsor:	Vice President, Finance and Administration
Approval Authority:	Algonquin College Executive Team
Date First Approved:	2012-05-16
Date Last Reviewed:	2020-11-26
Mandatory Review Date:	2025-11-26

PURPOSE

Algonquin College's information, technology systems and technology-related services are shared resources that are critical to teaching, learning, research, and business operations.

The purpose of this policy is to identify the responsibilities of College community members to protect College information and technology systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

SCOPE

This policy applies to:

1. All data and information, whether in digital, paper, audio or visual form;
2. All technology hardware and software used by the College whether on-premise, off-premise, in the cloud, or that connect to College IT systems;
3. All technology systems whether Information Technology (IT), Operational Technology (OT), Academic Technology (AT) or Internet of Things (IoT) technology;
4. All Algonquin College campuses, offices and other facilities; and
5. All learners, faculty, staff, contractors, volunteers, visitors, partners, vendors, and service providers that have access to College information or technology systems.

DEFINITIONS

Word/Term	Definition
Academic Technology (AT)	Any technology system designed to facilitate learning, such as a digital nursing training manikin.
Authorized User	A user authorized to use College IT systems.
College Community IT Users	Learners, faculty, staff, contractors, volunteers, visitors, partners, vendors, and service providers that have access to College information or technology systems.
Contractor	A company or person contracted to perform a service.

Cyber Security	The protection from cyber-attacks that disrupt, disable, destroy, or control technology systems, or steal or destroy information.
Cyber Security Incident	A security event that compromises the confidentiality, privacy or integrity of information, lessens the resiliency of a technology system or creates a life safety situation.
Data	Facts and statistics collected together for reference or analysis.
Identity Federation	An IT application's use of a centralized set of accounts and users. Also referred to as Single Sign On (SSO).
Information	Facts provided or learned about something or someone.
Information Security	The protection of information and IT systems from unauthorized access, use, disclosure, disruption, modification, or destruction, to provide confidentiality, integrity, and availability.
Information Security Incident	A security event that compromises the confidentiality, integrity or availability of information.
Information Sensitivity	The level of sensitivity of the information, normally Low, Medium or High.
Information Technology (IT) Resources	Information and IT systems of all types including hardware and software.
Information Technology (IT) System	The use of computers to store, retrieve, transmit, and manipulate information.
Information Technology (IT) System Custodian	A person that is responsible for overseeing, and/or operating and/or maintaining an IT System, which may include hardware and/or software.
Internet of Things (IoT) Technology	Interconnected digital devices with embedded sensors, software, and network connectivity that enables the collection and dissemination of useful business data. Information and IT systems of all types.
Learner	A prospective student; a lead or applicant; a registered student; a graduate; or an employee that is engaged in a learning activity with Algonquin College.
Operational Technology (OT) System	Any technology system that monitors and controls the physical state of a system, such as a power generation system.

Personal Information	Personal information means any data that can identify an individual, including but not limited to the individual's name, home addresses and email addresses, telephone numbers, age, sex, marital or family status, identifying number, race, national or ethnic origin, colour, religious or political beliefs or associations, educational and medical history, disabilities, blood type, employment history, financial history, criminal history, anyone else's opinions about an individual, an individual's personal views or opinions, and name, address and phone number of parent, guardian, spouse or next of kin.
Personal Health Information (PHI)	Identifying information about an individual relating to the physical or mental health of the individual or the provision of health care. Where it is held for purposes related to the provision of health care, the Ontario Personal Health Information Protection Act (PHIPA) governs the College's collection, use and disclosure of the information.
Personally Identifiable Information (PII)	Any data about an identifiable individual. Depending on the information in question, the Ontario Freedom of Information and Protection of Privacy Act (FIPPA) and the federal Personal Information Protection and Electronic Documents Act (PIPEDA) govern the College's collection, use and disclosure of the information.
Privacy Breach	A privacy incident that results in the confirmed access, use, copy, alteration or disclosure of personal information to an unauthorized party as well as the loss or theft of such information. Is also called a data breach.
Privacy Incident	An incident where personal information may have been collected, retained, used, altered, disclosed or disposed of in ways that do not comply with personal information protection requirements in statute, regulation and/or the College's policies and procedures.
Security Awareness and Training (SAT)	Teaching and learning related to information security, cyber security and information privacy.
Security Violation (Minor)	Any attempted or actual breach of College policy, standards or guidelines affecting information or technology systems, whether or not a compromise results (e.g., sharing a password or storing PHI on unapproved portable media).
Security Violation (Major)	Numerous or repeat minor violations; attempted or actual deliberate circumvention of security controls (e.g., hacking); attempted or actual breach of legislation or regulation (e.g., criminal code of Canada, PIPEDA).

Service Provider	A company that provides an IT related service, such as a Software as a Service (SaaS) application or other IT related services.
Software	The operating system and programs used by a computer.
Software Custodian	An IT system custodian that is responsible for overseeing, and/or operating and/or maintaining particular software.
Technology Types	Information Technology (IT) such as computing and networking systems; Operational Technology (OT) such as power generation systems; Academic Technology (AT) such as digital nursing training manikins; or Internet of Things (IoT) technology such as building environmental sensors.
Third Parties	Contractors, consultants, vendors, service providers and any other entities, including College partners, engaged by the College for the delivery of services or goods while either on the College's premises or not
User	Anyone who creates, stores, uses, shares, archives or destroys information or uses IT systems.
User Agreement	A set of rules that govern the use of College information, IT systems and other related assets.
User Credentials	A User ID for identification and proof for authentication, such as a password, a token or biometrics.
User ID	A unique identifying credential.
Vendor	A company that sells IT solutions, usually hardware and software.

POLICY

OVERVIEW

The goal of information security is to protect information and IT systems with an acceptable level of risk, achieved by implementing a set of controls including policies, standards, guidelines, procedures, practices, organizational structures, hardware, software, IT services, education and training.

1. IDENTIFY

1.1. Information Security Documentation Overview

College Information security documentation consists of the following hierarchical and related authoritative documents:

1. Information Security Policies, Standards, and Guidelines (PSG) Framework, which describes the relationship between the various document types;
2. Information Security Policy (i.e., this document); and
3. Information Security Directives (standards that provide detailed mandatory requirements in specific areas such as information classification, encryption and cloud security) including the procedures contained within.

1.2. Information Security Policy, Standards and Guidelines Framework

The College, through the ITS Cyber Security Unit, has created an overarching Information Security Policies, Standards and Guidelines (PSG) Framework, aligned with the globally adopted US National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), to categorize security controls within five primary functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

1.3. Information Security Governance

1.4.1 Management Responsibilities

1. While information security is everybody's responsibility, and while security specialists play an important role in helping make sure that security controls are properly designed, implemented, and functioning, overall decision making, responsibility and accountability rests with College management. The manager in charge of a school, department or sub business unit is responsible for the security of information and IT systems handled by the business unit, as well as the associated risks.
2. Managers must support information security efforts with their teams on a top-down basis. This typically includes but is not be limited to planning and discussion activities, provision of this policy to all employees, funding security safeguards where required, encouraging employee attendance at security and privacy training sessions, and inclusion of employee information security responsibilities in position descriptions. General security responsibilities expected of all employees will be developed by ITS and will be added to all position descriptions by the Human Resources Department.

3. Managers must provide this policy to all employees, contractors and service providers associated with their business unit. Alternatively, managers may refer to the location of where the policy has been published.
4. Managers must ensure that all of their employees receive mandatory annual information security and privacy training, as provided by the ITS Cyber Security Unit.
5. Managers must ensure that each employee's position description includes basic responsibilities related to the protection of information.
6. Managers must immediately notify the Manager, Information Security and Privacy of any actual or suspected security incidents or privacy breaches. Notification must be made via phone. In the event that the Manager of Information Security and Privacy cannot be reached, notify the Associate Director, IT Operations, ITS.

1.4.2 Employee Responsibilities

1. Employees must adequately protect information and IT systems in their care and custody at all times per this policy and related directives.
2. Employees must undertake annual, online information security and privacy training, as provided by the ITS Cyber Security Unit.
3. Employees must review this policy on an annual basis during annual security and privacy training.
4. Employees must immediately notify the Manager, Information Security and Privacy of any actual or suspected security incidents or privacy breaches.

1.4.3 Learner Responsibilities

1. Learners must adhere to this policy and related directives.
2. Learners must immediately notify the Manager, Information Security and Privacy of any actual or suspected security incidents or privacy breaches. Notification must be made via phone. In the event the Manager of Information Security and Privacy cannot be reached, notify the Associate Director, IT Operations, ITS.

1.4.4 ITS Chief Digital Officer Responsibilities

1. The ITS CDO or delegate(s) must specify in writing the assignment of IT system custodianship and related responsibilities. In most instances, IT system custodianship will be assigned to a manager within ITS. In some instances, IT system custodianship will be assumed by a school or departmental manager.

1.4.5 ITS Cyber Security Unit Responsibilities

1. The Manager, Information Security and Privacy is responsible for direction, guidance, creation of information security programs and services, as well as the creation and maintenance of information security and privacy charter, policies, directives, guidelines, and procedures.
2. The Manager, Information Security and Privacy, and delegate(s) may audit, inspect and investigate any College physical space housing technology systems, any technology or supporting system, any IT application whether on-premise or in the cloud, at any time.
3. Cyber Security Unit security specialists are responsible for assisting managers and IT system custodians with the security risk assessment of technology systems and the provision of security advice, guidance and recommendations.

1.4. Information Security Risk Management

In addition to the implementation of generally accepted good business practices and mandatory compliance security controls, the ongoing assessment of information and technology-related risks and application of additional risk mitigation measures is an important component of College risk management practices.

The ITS Cyber Security Unit facilitates the College information security risk assessment approach and methodology. The Manager, Information Security and Privacy must maintain alignment of the information security risk assessment approach with the College's Enterprise Risk Management (ERM) approach and risk management methodology to ensure that technology-related risks can be easily incorporated into ERM risk management models for executive-level review and approval.

IT system custodians must undertake risk assessments for new IT systems and whenever they undergo change.

Refer to the Information Security Risk Management Directive for detailed information and additional mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

1.5. Information Classification

The College's information classification scheme establishes different levels of information sensitivity based on information value and business impact from the loss of the information confidentiality, integrity and availability.

By identifying information with its sensitivity level, the College community that creates and shares information can protect the information with an appropriate set of pre-determined and consistently applied security controls throughout its lifecycle. This ensures the most efficient and cost-effective security protection approach.

All employees must classify and label all College information as per the classification scheme, at the time of creation or at the time of collection. This includes but is not limited to handwritten notes, Word documents, PDF documents, Excel spreadsheets, PowerPoint presentations, print outs, emails, videos and audio clips.

All employees must protect College information throughout its lifecycle as per this policy and its related Directives.

Refer to the Information Classification Directive for detailed information and additional mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

1.6. Third-Party Security

External third parties include but are not limited to IT infrastructure and application service providers, operations technology providers, academic technology providers and IoT providers. They are frequently contracted to provide and manage IT systems, either on-premise or off-site, in situations that often include the handling of College information, and thus can often present high, unacceptable security risks if not managed appropriately.

College managers wishing to contract third-party technology providers and solutions must:

1. Obtain Dean or Director review and approval to proceed
2. Obtain ITS review and approval before procurement
3. Identify the types of information (e.g. learner or employee personal information, credit card data, applied research data, system management data) that are involved to the data field level
4. Ensure that the requirements of College policy AA35 are met if learner records are involved
5. With ITS Cyber Security Unit assistance, undertake the following:
    a. Complete a Privacy Impact Assessment (PIA) if learner or employee personal information is involved;
    b. Complete a third-party information security risk assessment;
    c. Identify mandatory compliance requirements if subject to FIPPA, PHIPA, PIPEDA, or PCI DSS;
    d. Develop and document a system account management plan if an IT application is not identity federated; and
    e. Incorporate appropriate security and privacy clauses into contracts.

Refer to the Third-Party Security Directive for detailed information and additional mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

1.7. IT System Monitoring and Disclosure

To properly manage its information, technology systems and enforce security, the College may monitor, inspect, examine, view, log, block, and otherwise utilize or control any information stored on or passing through its technology systems as required. Criteria for exercising these duties may include (but are not limited to) investigation of malicious activity and prevention of security incidents. This examination may take place with or without the knowledge or consent of users. All learners and employees should expect that the information that they transmit or store, and the activities that they undertake on College technology systems and equipment will be subject to monitoring. Learners and employees who wish to send, receive or access sensitive personal information without monitoring by the College, should use their own technology systems and equipment, and should not send, receive or access such information using technology systems and equipment owned by the College.

The technology systems subject to College monitoring and examination includes, but is not limited to, College-owned computers and mobile phones, networks, electronic mail, voice mail systems, data storage systems, applications whether on-premise or in the cloud, printers, fax machines, operations technology, academic technology or IoT technology.

The information that the College may examine includes, but is not limited to, user log in and log out times, user geographical internet protocol (IP) location information, information transmitted and stored, systems and websites visited, system cookies, email content and email rules set, desktop phone numbers dialed and received, College-owned mobile phone telephone numbers dialed and texts, voice mail, fax data, system reports and system metadata.

The information that the College may remove from its IT systems at any time includes, but is not limited to, any information considered to be non-authoritative, plagiarized, duplicated, policy-violating, illegal, or otherwise puts the College at risk.

The College may use monitoring and examination results to support security investigations, police investigations, courts of law subpoenas, information access requests, College disciplinary proceedings,

and litigation among other uses. The College may disclose the results of any general or individual monitoring, including the contents and records of individual communications, to College officials, litigants, and municipal, provincial or federal law enforcement agencies. Use and disclosure of this information will be subject to applicable laws and College policies.

The College will not use monitoring or examination of the information described in this section for the purpose of routine monitoring of employee productivity or performance, but may use the information in the course of investigations in the workplace.

Past employees may not obtain copies of their College electronic files and College email communications. Exceptions in limited circumstances may be granted if approved by the area Vice President, Vice President of Human Resources and the Manager, Information Security and Privacy. Past employees may request copies of their College-owned mobile phone contacts if approved by the same officials.

Managers may request copies of their past employee's College electronic files and College email communications from ITS, to support continued business operations, if approved by the area Vice President and the Manager, Information Security and Privacy.

1.8. Acceptable Use of Information and IT Resources

The College's information and IT resources support its educational, instructional, learning, research, administrative and operational activities. The use of these resources is a learner and employee privilege, which is also extended to some members of the broader College community. Authorized users must undertake IT resource usage in a responsible, ethical, and legal manner respecting and adhering to policies and directives of the College; respecting local, provincial, federal and international laws; and respecting the rights of other users.

1. Authorized users of College IT resources, except for the use of guest Wi-Fi, must use a unique account User ID.
2. Before being issued a unique account User ID, users must agree to review and uphold this policy as well as the User Agreement appended to this policy (Appendix 2 – Algonquin College IT Resource User Agreement for Employees and Contractors). The employee or contractor must sign the User Agreement while being initially on-boarded. The User Agreement may be amended from time to time as deemed appropriate by the College, without requiring a change to this policy.
3. Authorized users must maintain the confidentiality of their passwords and the security of their accounts. This confidentiality and security does not provide authorized users with any expectation of privacy in their use of College IT systems, but rather facilitates authentication of the user.
4. Users must not access another user's account and related privileges.
5. Authorized users are solely responsible for all actions taken, including electronic messaging, while their account is being used. If a user suspects that their User ID has been compromised, or that their account has otherwise been improperly accessed, the user must immediately report the suspected breach to the Manager, Information Security and Privacy.
6. The sharing of access through peer-to-peer technology, network access hosting, proxy hosting, Bluetooth, Wi-Fi, or any other technology must not take place on College networks except when it supports academic learning and is pre-authorized by the responsible manager.

7. Information providers must use official College data from the school or department that is responsible for creating and maintaining that data. For example, the Registrar's Office (RO) is responsible for timetable information. Information providers must use RO data sources rather than creating their own.
8. Given the high risk of accidental or deliberate unauthorized disclosure, users must not use portable media devices, including USB drives and portable hard drives to store sensitive College data, including learner and employee personal information, unless ITS-approved encryption methods are used for protection. Furthermore, portable media devices must not be used under any circumstance to store personal health information (PHI).
9. The use of the College's information and IT resources for personal gain, commercial or fraudulent purposes is a major violation of this policy as well as the College's Conflict of Interest Policy (HR12) unless the user has submitted and received an approved conflict of interest disclosure.
10. The use of the College's IT resources to engage in activities that violate a person's right to work and study in an environment free from harassment, hate and discrimination is a major violation of this policy as well as the College's Employee Code of Conduct Policy (HR18) and Respectful Workplace Policy (HR22).
11. The use of the College's IT resources to engage in activities related to sexual assault or sexual violence is a major violation of this policy as well as the College's Sexual Assault / Sexual Violence Policy (SA16).
12. The use of the College's IT resources to engage in activities that violate copyright is a major violation of this policy as well as the College's Copyright Policy (AA34).
13. The use of the College's IT resources to access, create, publish or communicate information that is obscene, pornographic or otherwise offensive is a major violation of this policy. However, as the College recognizes and supports academic freedom per the Academic Freedom Rights and Responsibilities Policy (RE07), it is not considered an offence to seek out information that may be considered offensive, provided that is undertaken for specific and legitimate research purposes and provided that it does not violate the Criminal Code of Canada.
14. Any attempt to circumvent local, provincial, federal or international laws using College IT systems is a major violation of this policy and may result in litigation against the offender by the authorities. If such an event should occur, the College will fully comply with the authorities to provide any information necessary in support of the litigation process.
15. Violations of this policy could result in a Criminal Code of Canada offence. Should this occur, the College will fully comply with local, provincial and federal police and other judicial authorities to provide any information necessary in support of criminal processes.
16. The College may temporarily or permanently close a user account, or access, manage, move, or delete College information associated with an account on College devices, and recover College owned devices as required.
17. The College provides numerous computer labs throughout its campuses. All learners entitled to use the computer labs must comply with the Computer Lab Regulations provided in Appendix 3.
18. A violation or attempted violation of the provisions of this policy may result in disciplinary action. Disciplinary actions range from a reprimand, either oral or written, to loss of account privileges, to maximum penalties afforded under College policies, which includes expulsion of a learner from the College or the termination of employment for employees.

2. PROTECT

Effective information security uses a three-layer protection model. Managers and IT custodians must only implement security controls in a particular situation or for a particular IT system if they fall into one of the following three defence layers; otherwise, College resources, including human and monetary, must not be expended. The purpose is to avoid implementing security controls where they are not warranted.

1. Generally accepted good business security practices and 'security hygiene' practices (e.g. use of strong passwords, data encryption, anti-malware software and employee security awareness and training).

2. Legislative and regulatory requirements (e.g. FIPPA, PHIPA, PIPEDA, PCI DSS requirements for reporting privacy breaches).

3. Formal risk assessment results (e.g. identification of unacceptable phishing attack risks and recommended additional security controls).

2.1. Information Security Awareness and Training

Information security awareness and training (SAT), which promotes learning and appropriate behaviour relative to the protection of information and technology systems, is foundational to the College's information security program, its legislative compliance requirements, and the College's business objectives.

1. The Manager, Information Security and Privacy must establish and maintain a College-wide, mandatory participation information security awareness and training (SAT) program, comprising a variety of learning opportunities, covering employees, contractors, and third parties.
2. All College community members must participate in information security and privacy training on a regular and routine basis.
3. Employees must undertake mandatory online training, and review this policy, on an annual basis.

Refer to the Information Security Training and Awareness Directive for detailed information and additional mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

2.2. Personnel Security

Personnel security is a fundamental practice that establishes a foundation of trust for individuals that require access to sensitive information. It includes security-screening activities and the binding of individuals to confidentiality agreements. It also includes the provision of security clearances to College employees that work on contract for the Canadian federal government.

1. All College employees and contractors must sign the College's standard Confidentiality Agreement, as per Appendix 1, before their employment or provision of services.
2. All new College employees and contractors expecting to have extensive access to highly sensitive learner, employee, or business information, or extensive access to IT systems must undergo and pass suitable security screening before employment or provision of services.

Suitable security screening includes valid federal government enhanced reliability or higher security clearance if the employee already has this, or an Ottawa Police Level Two (2) Criminal Record and Judicial Matters Check (CRJM) or other equivalent screening as approved by the Manager, Information Security and Privacy. The College area must incur any associated costs. This requirement is applicable, but not limited to, the following roles:

a. Executives,
b. Executive Assistants,
c. Deans and Directors,
d. ITS employees and contractors,
e. Human Resources employees and contractors,
f. Finance employees and contractors,
g. Health Services employees and contractors,
h. Registrar's Office employees and contractors,
i. Security employees and contractors,
j. Facilities Management employees and contractors that are provisioned with extended facilities access,
k. Cleaners that have access to office spaces, and
l. Others, as identified by the President, Vice Presidents or the Chief Digital Officer.

3. Managers overseeing contracts with the Canadian federal government that require employee security clearances must ensure that the security clearances are established before any contract work is started, by contacting the ITS Manager of Information Security and Privacy.

2.3. Physical Security

The College creates a significant amount of sensitive information, both paper and digital form, including but not limited to learner and employee sensitive personal information. It also has a significant amount of IT assets, including an IT data centre, numerous IT closets located through its campuses and computers located in virtually every room. Most of the College's physical space, containing sensitive information and computers, is vulnerable to improper access given the nature of its 24/7 publicly accessible buildings. All of this results in College information and its technology systems being highly vulnerable to improper access if not properly secured at all times.

1. Managers must protect the physical spaces that contain IT systems and computers for which they are responsible.

Refer to the IT Physical Security Directive for detailed information and additional mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

2.4. Software Security

Managers that act as, or have delegated the role of software custodian within their business units, must ensure that software, whether on-premise common-off-the-shelf (COTS) software, custom-developed software, or Software as a Service (SaaS), is acquired, developed, configured and maintained with adequate security controls to protect the software and associated information that it is processing. In most instances, but not all, ITS managers will act as software custodians on behalf of the College.

1. Given the high inherent security risks, software acquired by the College or deployed by third parties must only be COTS or SaaS, and must not be custom developed software, unless used to

support academic software development learning, or unless authorized by the Chief Digital Officer.
2. All software acquired and deployed into a production environment must be approved by the Dean or Director and by the ITS Chief Digital Officer.
3. All software acquired must have identity federation capability rather than creating an independent account schema, unless a waiver is obtained on an exception basis only from the Chief Digital Officer.
4. Software must not be acquired using corporate credit cards unless a waiver is obtained, on an exception basis only, from the Chief Digital Officer.
5. Software custodians must maintain separate development, testing, staging and production environments for business critical and custom-developed software.
6. Software custodians are accountable for ensuring that security assessments are undertaken with assistance of the ITS Cyber Security Unit; for ensuring that regular patching and other corrective measures are applied; and for securely disposing of no longer required custom-developed software.
7. Managers must adhere to software copyright compliance requirements when acquiring and deploying software.
8. When software requires integration with other software to exchange data and information, software custodians must use the College's official application programming interface (API) manager, as managed by ITS.

2.5. IT Infrastructure Security

The College's IT Infrastructure, including but not limited to networking and Wi-Fi technology, servers, and supporting technologies, must be adequately protected to provide a secure IT infrastructure platform to support the College's teaching, learning, academic and business operations, research and service delivery.

1. The ITS Manager, Infrastructure and Network Operations, must undertake the following practices:
    a. Implement networking devices and build new servers using commercial system hardening guides, followed by vulnerability testing, before placing them into a production environment;
    b. Architect the networking and server environments with sufficient segregation and progressively restrictive security zoning;
    c. Ensure that operating system versions are officially supported;
    d. Maintain a regular and routine network device and server operating system security patching regimen to help reduce security vulnerabilities and cyber risk; and
    e. Implement strong, multi-factor authentication for ITS Infrastructure employees and contractors to access networking and server technology.

2. The Manager, Information Security and Privacy must implement network security technology that identifies and analyzes computing devices attaching to the network and rejects attachment of those that are determined to be insecure (e.g., those without current anti-malware software).

2.6. Computer Security

The College's many computing devices, including but not limited to desktop, laptop and tablet computers, must be adequately protected to provide a secure computing environment to support the College's teaching, learning, academic and business operations, research and service delivery.

The ITS Manager, Endpoint Services, must undertake the following practices:

a. Prepare, maintain and deploy employee and learner loaner computers with hardened operating systems, whole disk encryption and the most current version of enterprise security software;
b. Ensure that operating system versions are current, supported and no older than one major version old. Any exceptions must be approved by the Chief Digital Officer or delegate;
c. Ensure that enterprise computers are maintained with the latest operating system and security patches to help reduce security vulnerabilities and cyber risk;
d. Implement strong, multi-factor authentication for ITS Desktop employees and contractors to access the centralized golden image production environment;

2. All computers must undergo standardized ITS imaging before being deployed; and
3. Users of College computing devices must protect them from loss and theft at all times, including but not limited to storing them in locked spaces or securing them using computer locks when not being used, and by not storing them in unattended vehicles.

2.7. Email, Texting and Instant Messaging Application Security

The College provides all of its learners, alumni, full and part-time employees, and some contractors with Microsoft email accounts. Email contains significant sensitive information, including learner and employee personal information. Therefore, users must manage and protect their email accounts and sensitive information accordingly.

While mobile phone texting and instant messaging applications provide useful communications means, they do not meet the requirements for official records management, including the ability to service FIPPA Freedom of information access requests.

1. Full and part-time employees and contractors must use a College provided email account for communications to conduct College business.
2. Learners, while officially enrolled, must use a College provided email account for communications to conduct College business, whenever possible.
3. Employees including retirees may not keep or use their email accounts after employment ceases.
4. Learners may keep their College email account for up to two years following graduation. This may be extended at the College's discretion.
5. Learner email accounts may be disabled after one year of inactive use, to reduce security risks.
6. Employees must communicate with learners using their College provided email accounts. They may use learners' personal email accounts before they receive their College provided email account, or for backup or emergency purposes; however, they must not communicate sensitive personal information using the learner's personal email accounts unless email encryption is used.
7. Contractors may be provided with a College provided email account if approved by a manager. The network and email accounts must have a defined end date of one year or less, which may be renewed.

8. Employees and contractors with College provided email accounts must use email encryption, if available, to communicate sensitive information to others.
9. Employees must not use mobile phone texting and messenger applications to replace email for official College communications.
10. While collecting records in response to an access to information request, employees must search for and produce any relevant records from instant messaging and personal email accounts.
11. Individuals using their own personal computing devices and mobile phones to access College provided email accounts must implement the security controls identified in Appendix 2: Algonquin College IT Resource User Agreement for Employees and Contractors.
12. Employees and contractors with College provided email accounts must use the following automatically generated email disclaimer at the bottom of all emails:

    This email is intended solely for the addressee(s) and is Confidential. If you received this in error, any disclosure, copying, or distribution is prohibited. Please reply and inform the sender and delete all copies. Thank you.

2.8. Bring Your Own Device (BYOD) Security

The College provides computing devices for all full-time employees, some part-time employees, some contractors, as well as mobile phones for administrators and other employees. ITS has deployed these devices with standardized security controls to adequately protect College information and the IT systems that they access.

1. Full-time employees must use a College provided computer at all times to conduct College business, including while working at the office, at home and while travelling on College business.
2. Part-time employees must use a College provided computer to conduct College business if the employee will be handling a significant amount of sensitive learner, employee or other information.
3. Managers must provide contractors with a College provided computer to conduct College business if the contractor will be handling a significant amount of learner, employee, or other information.
4. Individuals using their own personal computing devices and mobile phones to access College information and IT systems must implement the security controls identified in Appendix 2: Algonquin College IT Resource user Agreement for Employees and Contractors.

Refer to the Bring Your Own Device (BYOD) Security Directive for detailed information and additional mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

2.9. Cloud Security

As part of a natural IT evolution, the College continues to migrate from on-premise IT solutions to those in the cloud. These solutions include information storage, software applications and IT infrastructure solutions. Cloud computing, while no doubt provides increased efficiencies and cost-effectiveness, can also present new and increased security risks if not carefully deployed and managed.

1. If employees use cloud storage, then they must use College provided OneDrive, SharePoint Online, or Teams applications to store College information. Employees must not use personal OneDrive, Google Drive, Dropbox, Box or other cloud storage solutions.

Refer to the Cloud Security Directive for detailed information and mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

2.10. Internet of Things (IoT) Security

IoT is the fast-growing network of interconnected digital devices with embedded sensors, software, and network connectivity that enables the collection and dissemination of useful business data. As with most organizations, the College continues to deploy IoT to modernize its business. However, without adequate security, malicious actors can compromise IoT environments, putting College information and IT systems, and life-safety at risk.

College IoT is segmented into the following:

- Corporate IoT, which includes College-owned and managed devices such as smart audio-visual equipment;
- Building Management IoT, which includes specialized environmental sensing devices, power generation systems, operational technology and industrial control systems (ICS); and
- Academic IoT, which includes learning IoT systems and classroom digitized systems.

1. Managers must submit all IoT system (including contracted systems) deployment requests to ITS for approval, before any form of deployment (e.g., demonstration, testing, production).
2. Managers deploying IoT must identify security requirements along with a security plan, assisted and endorsed by the ITS Cyber Security Unit.
3. Managers must ensure that IoT systems' software under their control are kept current and security patched on a regular and routine basis.
4. The Manager, Infrastructure and Network Operations, must connect IoT systems to appropriately segregate and controlled network segments, which must be security monitored to identify abnormal traffic and emergent cyber risks.
5. Learners (with the exception of residents), employees, and contractors must not connect consumer IoT systems (e.g., smart speakers, smart televisions) to the College's networks or AC Secure Wi-Fi (Guest Wi-Fi excepted) without Management and ITS prior approval.

2.11. Identity & Access Management (IAM) Security

College Information is an important strategic asset. Personal and third party business information is entrusted to the College and must be adequately protected. Therefore, Managers must ensure that College IT digital identities, system accounts, passwords, password managers and access control to applications and information are carefully controlled.

Refer to the Identity and Access Management (IAM) Security Directive for detailed information and additional mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

2.12. Encryption

Encryption is the process of encoding information in such a way that only authorized individuals can access it.

IT system custodians and users must use approved encryption methods, techniques, ciphers and algorithms to protect sensitive information in the following circumstances:

1. When information 'at rest' is vulnerable to improper physical and digital access. This includes, but is not limited to, information stored in portable computers, external hard drives and USB drives, the information in files stored in data storage areas that have extensive user access, and SaaS application databases within shared 'tenants.' Solutions include file, database and whole disk encryption.
2. When information 'in motion' is vulnerable to improper eavesdropping access. This includes, but is not limited to, sensitive information transmitted through open and public networks and Wi-Fi networks. Solutions include Transport Layer Security (TLS), virtual private networking (VPN), and network encryption.

Refer to the Encryption Security Directive for detailed information and additional mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

3. DETECT

3.1. Security Logging and Monitoring

IT system custodians must ensure that all College IT systems including networking equipment, servers, computers and application systems (both on-premise and SaaS) log operational and security-relevant information that a minimum includes the following, if feasible:

1. User session activity including user IDs, log in and log off date and time, failed access attempts, and account lockouts;
2. Source and destination IP addresses;
3. Applications accessed and changes made to user privileges;
4. Files accessed, Internet services and websites accessed;
5. Changes made to system files;
6. System errors reported; and
7. System start-up and shutdown dates and times.

IT system custodians must keep IT system log data for a minimum of one year.

IT system custodians must ensure that business-critical systems including networking equipment, servers, computers and primary application systems (including on-premise and SaaS), provide log data to the ITS security operations centre (SOC) security incident and event monitoring (SIEM) system for ongoing security analysis and alert generation.

4. RESPOND

4.1. Security Incident Response

While the College strives to prevent information and cyber security incidents and privacy breaches, they will inevitably occur. Therefore, managers and employees must plan for and respond accordingly.

Employees, contractors and third parties must immediately notify the Manager, Information Security and Privacy upon becoming aware of a suspected or actual information security incident, cyber security incident, or privacy breach, whether minor or major.

The Chief Digital Officer must ensure that detailed security incident response plans and processes are developed, implemented, tested and maintained to ensure that the College is adequately prepared to respond to significant information security or cyber security events.

The Chief Digital Officer must develop and maintain an in-house cyber incident response team (CIRT) that will provide incident assessment, containment and control, resolution, and communications coordination in the event of a significant information security or cyber security incident.

The Chief Digital Officer must establish an external, third-party cyber-incident assistance retainer to ensure that external cyber incident assistance is readily available if required.

IT system custodians must establish a security response plan, assisted and endorsed by the ITS Cyber Security Unit, for the business-critical IT systems that they manage.

Refer to the Cyber Incident Response Plan (CIRP) Directive for detailed information and additional mandatory requirements.

Refer to the Information Privacy policy (***AD24***) for detailed information and mandatory requirements associated with privacy breach management and response.

4.1. Policy Enforcement

Where a user has violated this policy, the Manager, Information Security and Privacy, together with the Manager involved, and, where required, the College officials referred to in the Employee Code of Conduct Policy (HR18), must jointly determine suitable disciplinary action, which includes up to and including expulsion of a learner from the College or the termination of employment for employees, for major violations.

5. RECOVER

5.1. IT Disaster Recovery

Numerous perils, including hardware and software failures and environmental disasters, can affect the availability of College information and IT systems, at any time. While the College strives to prevent these from affecting business operations, they will inevitably occur. Therefore, managers and employees must be prepared to plan for and respond accordingly.

The Chief Digital Officer must ensure that detailed IT disaster recovery plans and processes are developed, implemented, tested and maintained to ensure that the College is prepared to respond to a significant loss of information or IT system availability.

Refer to the IT Disaster Recovery Planning and Recovery Directive for detailed information and additional mandatory requirements. https://www.algonquincollege.com/its/information-security-services/

PROCEDURES

Procedures for implementing, maintaining and enforcing these policies are contained with the supporting Information Security Directives. Refer to the "RELATED INFORMATION SECURITY DIRECTIVES" section.

SUPPORTING DOCUMENTATION

Appendix 1 Algonquin College Confidentiality Agreement for Employees and Contractors
Appendix 2 Algonquin College IT Resource User Agreement for Employees and Contractors
Appendix 3 Computer Lab Security Regulations

RELATED POLICIES

AA34 Copyright
AA35 Confidentiality of Student Records
AD02 Freedom of Information
AD09 College Corporate Image
AD19 Fraud Prevention
AD20 Enterprise Risk Management
AD23 Internal Control
AD16 Payment Card Industry Data Security Standards
AD24 Information Privacy
HR12 Conflict of Interest
HR18 Employee Code of Conduct
HR22 Respectful Workplace
HS15 Food and Drink in Labs and Shops
RE03 Research Involving Human Subjects
RE05 Intellectual Property
RE07 Academic Freedom Rights and Responsibilities
SA07 Learner Conduct
SA16 Sexual Assault / Sexual Violence

RELATED INFORMATION SECURITY DIRECTIVES (CURRENTLY IN DEVELOPMENT)

Directives are located here: https://www.algonquincollege.com/its/information-security-services/
ISD01 Information Classification
ISD02 Information Security Risk Management
ISD03 Information Security Awareness and Training
ISD04 Personnel Security
ISD05 IT Physical Security
ISD06 Threat and Vulnerability Management
ISD07 Identity and Access Management
ISD08 Encryption
ISD09 Cloud Security
ISD10 Bring Your Own Device Security
ISD11 Third-Party Security
ISD12 Cyber Incident Response Plan
ISD13 IT Disaster Recovery Planning and Recovery

RELATED MATERIALS

Information Security Policies, Standards, Guidelines (PSG) Framework

IT01: Appendix 1

ALGONQUIN COLLEGE CONFIDENTIALITY AGREEMENT FOR EMPLOYEES AND CONTRACTORS (THE "AGREEMENT")

I, _____, hereby acknowledge and agree that:

1. I owe certain contractual, common law and statutory duties of confidentiality with respect to Confidential Information, which I receive, access, collect or otherwise process in the course of my relationship with The Algonquin College of Applied Arts and Technology (the "College"). The purpose of this Agreement is to confirm and acknowledge those duties.

2. For the purposes of this Agreement, "Confidential Information" means any information of a confidential nature which relates to the business of the College and any affiliated organization, its learners, faculty, staff, contractors, volunteers, visitors, partners, vendors, and service providers, including, without being limited to, the following:

a. Confidential methods of operation, which includes all information relating to unique business or marketing programs, research, strategies, products, methods, techniques, concepts, formulas, documentation, service systems, security of information and systems, and trade secrets;
b. Sales and pricing policies;
c. Intellectual property including software, industrial designs, and products;
d. Customer, client, alumnus, donor, and supplier lists;
e. Financial information including costs, sales, income, profits and other similar information;
f. Personnel information about learners, employees, contractors, donors;
g. For the purpose of this Agreement, Personal information means any data about an identifiable individual, including but not limited to the individual's name, home addresses and email addresses, telephone numbers, age, sex, marital or family status, identifying number, race, national or ethnic origin, colour, religious or political beliefs or associations, educational and medical history, disabilities, blood type, employment history, financial history, criminal history, anyone else's opinions about an individual, an individual's personal views or opinions, and name, address and phone number of parent, guardian, spouse or next of kin.

3. Notwithstanding the foregoing, Confidential Information, except Personal Information, shall not include any information which:

a. I was in the possession of or knew about, without any obligation to keep it confidential, before it was disclosed to me by the College;
b. is or becomes public knowledge through intentional disclosure by the College;
c. is or becomes public knowledge through no fault of my own;
d. is independently developed by myself outside the scope of my engagement and/or duties to the College;

e. is intentionally disclosed by the College to another person without any restriction on its use or disclosure; or

f. is or becomes lawfully available to me from a source other than the College.

4. I acknowledge and agree that in performing the duties and responsibilities of my relationship with the College, I will become knowledgeable with respect to a wide variety of Confidential Information which is the exclusive property of the College, the unauthorized disclosure of which could cause irreparable harm to the College.

5. I therefore agree that during and following the termination of my relationship with the College for any reason, I am under an obligation to maintain confidentiality in the Confidential Information, and I shall not disclose the Confidential Information to any unauthorized persons, except in the course of carrying out authorized activities on behalf of the College or with the express and authorized consent of the College, or otherwise as required by law.

6. I further acknowledge that the College is bound by the provisions of the Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Health Information Protection Act (PHIPA), and the Personal Information Protection and Electronic Documents Act (PIPEDA). I acknowledge and agree that I have an obligation to adhere to these laws in all respects in the course of carrying out my duties on behalf of the College.

7. I further acknowledge and agree that I shall review and obey all applicable policies of the College relating to confidentiality and privacy, as amended or as may be introduced by the College in the future, including but not limited to policies AA35 (Confidentiality of Student Records), AD02 (Freedom of Information), AD16 (Payment Card Industry Data Security Standards), AD18 (Social Media Account Management), AD24 (Protection of Privacy) and IT01 (Information Security).

8. I understand and acknowledge that should I breach any of my obligations under this Agreement, I will be subject to immediate disciplinary action, up to and including the termination of my relationship with the College.

9. My statutory, common law and contractual obligations of confidentiality, including those described in this Agreement, shall survive the termination of my relationship with the College, howsoever caused.

10. Upon termination of my relationship with the College for any reason, I acknowledge and agree that I shall immediately surrender all Confidential Information in my possession or control to the College, and delete copies of the same, as applicable.

11. If I am not otherwise an employee of the College, this Agreement shall not be construed to give rise to an employment relationship.

12. If any part of this Agreement is or should be declared to be void or unenforceable by a court of competent jurisdiction, it shall be severed to the extent of the invalidity, and the remaining provisions or parts thereof shall continue in full force and effect.

13. This Agreement shall be subject to the laws of Ontario and the federal laws applicable therein.

14. I acknowledge that I have read and understand the terms of this Agreement. I specifically acknowledge that I have had an opportunity to seek independent legal advice at my own expense prior to executing this Agreement. My signature acknowledges my agreement to the terms and conditions as outlined above in the Agreement.

Signed this _____day of _____ 20__.

_____

(Print Name)

_____

(Signature)

(Provide one signed copy to the Employee/Contractor and keep one copy in the Manager's office)

IT01: APPENDIX 2

ALGONQUIN COLLEGE IT RESOURCE USER AGREEMENT FOR EMPLOYEES AND CONTRACTORS

Managers must keep copies of these signed agreements. Digitized copies may be kept within Workday.

On being issued an Algonquin College account User ID and email account, I agree that:

GENERAL

1. I will not apply for a User ID under pretenses.
2. I am the sole person authorized to use my User ID.
3. I am solely responsible for all actions taken using my User ID.
4. I will not allow others to use my User ID.
5. I will use strong passwords for my College User ID and applications that meet the College's Information Security Policy (IT01) and related Directive password creation requirements.
6. I will not use College IT resources for personal gain, commercial or fraudulent purposes.
7. I will not examine, copy, modify or delete information belonging to other users without prior consent.
8. I will not make any unauthorized, deliberate action that damages or disrupts an IT resource, alters its normal performance, or causes it to malfunction.
9. I will report any suspected or actual security violation, security incident, privacy breach or criminal act to the Manager, Information Security and Privacy or by sending an e-mail to infosec@algonquincollege.com.
10. I further acknowledge that the information transmitted or stored, and the activities undertaken on College technology systems and equipment may be subject to monitoring. The College will not use monitoring or examination of the information described in this paragraph for the purpose of routine monitoring of employee productivity or performance, but may use the information in the course of investigations in the workplace.

COMPUTING AND NETWORKING SECURITY

1. I will protect my College provided computer at all times from loss and theft.
2. I will use a College provided computer at all times to conduct College business, including while working at the office, at home and while travelling on College business, if I am a full-time employee.
3. I will use a College provided computer at all times to conduct College business, including while working at the office, at home and while travelling on College business, if I am a part-time employee or contractor and will be handling a significant amount of sensitive learner, employee or other information.
4. If using a personal computing device (e.g., desktop, laptop, tablet) to access College IT resources, I will ensure that it has whole disk encryption turned on, its operating system and anti-malware software is kept current, and it is not connected to any other network at the same time while connected to the College network.
5. If using a personal computing device (e.g., desktop, laptop, tablet, home computer), I will ensure at the end of my employment or contract that all information is returned to the College and any copies or remnants are securely destroyed.
6. I will use a password enabled screen saver set to a period of inactivity (15 minutes or less).

7. I will not use an unencrypted USB drive or unencrypted external hard drive to store sensitive College information.
8. I will not attempt to access IT resources that I am unauthorized to use or attempt to secure a higher level of user privilege within applications, other than what I have been authorized.
9. I understand that Microsoft OneDrive is the only official information cloud storage system for College use. I will not use third-party 'cloud' information storage services (e.g., personal OneDrive account, Dropbox, Google Drive) for the storage of College information.

EMAIL

1. I am solely responsible for all electronic mail originating from my User ID, even though I may share my e-mail account with an assistant or authorized user using the "delegated access" function.
2. I will only create messages that are necessary for the conduct of College business using my College provided e-mail account, although I may send and receive limited and reasonable non-College personal messages which are incidental to and do not interfere with the primary business use of the College's electronic messaging systems. I understand that such messages must still comply with this policy in all respects.
3. I will communicate with learners using their College provided email accounts. I may use learners' personal email accounts, either before they receive their College provided email account, or for backup or emergency purposes; however, I will not communicate sensitive personal information using the learner's personal email accounts unless email encryption is used.
4. I will not forge or attempt to forge electronic messages.
5. I will not send unwelcome, unwanted, offensive, intimidating, derogatory, hostile, threatening, pornographic or otherwise inappropriate messages to another user.
6. I will not send unsolicited 'for-profit' messages or chain letters.
7. I will not send unauthorized network broadcast messages.
8. I will not send solicitation emails to external recipients that do not have a formal business relationship with the College. I understand that this 'spam' could violate the Canadian Anti-Spam Legislation (CASL) and put the College at reputational and legislative compliance risk.
9. I will be careful not to misdirect emails to unintended recipients, particularly emails containing sensitive information. I understand that this could lead to a serious privacy breach.
10. I will not send unencrypted Word or Excel email attachments containing significant sensitive learner or employee information.
11. I will be careful not to click on suspicious e-mails, including phishes, but will instead use my "Report Phishing" email ribbon icon, when possible, to report and securely delete the suspicious emails.
12. I will include the following notice at the bottom of all my College emails: *"This email is intended solely for the addressee(s) and is Confidential. If you received this in error, any disclosure, copying, or distribution is prohibited. Please reply and inform the sender and delete all copies. Thank you."*

MOBILE PHONES

1. I understand that Apple iPhone is the College's preferred mobile phone technology and that Android or other mobile phones can only be purchased, on an exception basis, with the review and permission of the Manager, Information Security and Privacy.
2. I will always use a minimum of a six-digit PIN to protect access to my mobile phone, including for College-owned mobile phones as well as personal mobile phones used to access College IT resources. I will not share my six-digit PIN with anyone.

3. I will not use a 'jail-broken' or 'rooted' (weakened operating system) mobile phone to connect to the College network.
4. When using a personal mobile phone to access College IT resources, I will ensure that its operating system is kept current, and it has anti-malware software that is kept current.
5. I understand that Mobile phone text messaging must only be used for limited operations requirements and should not be used to replace corporate email messaging, to ensure that the College maintains official records in support of information access requests.
6. I will only create text messages that are necessary for the conduct of College business using my College provided mobile phone, although I may send and receive limited and reasonable non-College personal text messages which are incidental to and do not interfere with the primary business use of the College's electronic messaging systems. I understand that such messages must still comply with this policy in all respects.

I have read, understood and agreed to use my account(s) per this User Agreement.

I accept full work-related, professional and legal responsibility for all of my actions while using the College's IT resources.

_____
Employee/Contractor Name (Print)

_____
Employee/Contractor Signature

_____
Date (DD/MM/YYYY)

(Provide one signed copy to the User and keep one copy in Manager's office)

IT01: Appendix 3

COMPUTER LAB SECURITY REGULATIONS

Algonquin College learners are required to follow these regulations when using lab computers. Failure to do so can lead to disciplinary action, which may range from reprimand, either oral or written, to loss of account privileges, to maximum penalties afforded under College policies, which could include expulsion of a learner from the College.

1. Lab Administrators must post these regulations within each computer lab.
2. Lab computers are provided solely for academic teaching and learning purposes. They must **not** be used for recreational, commercial or other purposes.
3. Lab computers must only be used by College learners and employees.
4. All users must produce and prove personal identity if requested by campus security.
5. Users must respect other users in the lab. No loud talking or other disturbances are permitted.
6. Users must not use audio amplification devices other than earphones or headphones.
7. Users must not consume food or drink within computer labs as per College's Food and Drink in Labs and Shops policy (HS15).
8. Users must not alter computer configurations.
9. Users must only use College provided software applications.
10. Users must not access offensive, intimidating, derogatory, hostile, threatening, pornographic or otherwise inappropriate content.
11. All users must logoff computers after use.
12. Technical issues should be reported to a Lab Administrator or the ITS Service Desk at extension 5555 or 5555@algonquincollege.com.
13. Users with complaints about other users should be reported to Security Services at extension 5000.
14. Actual or suspected computer security violations should be reported to infosec@algonquincollege.com.