IT SECURITY POLICY

1. PURPOSE/ RATIONALE

This IT Security Policy ("Policy") outlines, at a high level, the expectations for maintaining the security of Humber's *information systems*, whether owned, leased or managed by a 3rd party (Hosted or cloud) and is guided by institutional security requirements specific to Humber's current operating environment and projected threat landscape.

This policy will strive to ensure the *confidentiality*, *integrity* and *availability* of the Information and data assets (hereafter referred to as Information) that support the business processes while taking into account the following desired outcomes:

- Minimize business information risks
- Preserve the trust of our students, staff and community,
- Ensure our services are securely delivered and available,
- Meet our legal and regulatory obligations, and
- Ensure emerging technologies are delivered in a secure fashion

2. OBJECTIVES AND PRINCIPLES

Objectives

Humber's IT Security objective is to establish the appropriate level of controls to manage security risks while enabling the Academic delivery and business operations. Humber achieves this objective through the design, deployment and operation of the IT Security Program in alignment with the following:

- Humber's risk thresholds
- Industry standards and best practices
- Regulatory and contractual requirements

Principles

- *Security Governance* **—** Personal accountability and responsibility for IT Security are incorporated in Roles and Responsibilities that ensure that every individual applies the applicable information security policies, principles, procedures and practices in their daily activities.

- *Security Control Measures* **—** Information security policies, standards, guidelines and procedures are developed to communicate security requirements and guide the selection and implementation of security control measures.

- *Continuous Awareness and Education* **—** Information security education, training and awareness programs ensure that users are aware of security risks and concerns and are equipped to apply organizational security policies and principles.

- *Protecting Security of Assets* **—** Information assets are classified according to their criticality to the organization enabling an appropriate level of protection. Information assets are to be used for the intended business purpose only. (See Data Governance Policy)

- *Legislative and Regulatory Compliance* **—** Legal, regulatory and contractual requirements are identified, documented and followed.
- *Measure and Monitor (Continuous improvement)* **—** Continual improvement requires measuring and monitoring the effectiveness and efficiency of IT Security program and making sure it is in accordance with the IT Security Policy.

3. SCOPE / AUDIENCE

The scope of IT Security includes all information and technology assets belonging to or managed by Humber located within our facilities, service provider facilities (e.g. Cloud) and the clients accessing these assets. Clients include but are not limited to:

- All employees (Faculty and Staff)
- All students and learners
- All suppliers, contractors and guests that use the Humber network
- All guests (Any external person or entity; this includes members of the public, retirees, event attendees, prospective students, alumni, advisory groups, varsity teams, etc.).

4. DEFINITIONS

- *Information*: Timely and accurate data organized and presented in a way that gives it meaning/relevance leading to increased understanding or reduced uncertainty.
- *Data*: Information in a raw or unorganized form (such as letters, numbers, symbols, or graphics) that refer to, or represent, conditions, ideas, or objects.
- *Employee:* Any individual (not an independent business) providing value to Humber on a regular or semi-regular basis in exchange for compensation.
- *Humber:* The Humber College Institute of Technology and Advanced Learning, and the University of Guelph-Humber; a post-secondary, educational institution in Ontario with multiple community service programs.
- *Student:* Any person actively enrolled in a Humber course including individuals in fully online courses and people using a Humber community service.
- *Learner:* Any person actively enrolled in Real Estate Education Program (REEP).
- *Supplier:* An independent business providing value to Humber (also known as a "vendor", "contractor", "strategic partner", and/or "consultant"). Examples include a cloud service provider, etc.
- *Client:* Any individual or entity (includes students, employees, suppliers, and guests) using one or more technical services at Humber (also known as a "Data User").
- *IT Security Standards:* Details and specifications that define the quality of the IT Security controls derived from the Information Technology Security Control Framework and that can be used as a measure.
- *IT Security Program*: The agreed projects to be undertaken to remediate the IT Security gaps in standards and processes and to attain the desired maturity level.

5. ROLES AND RESPONSIBILITIES

Humber will act appropriately to preserve the confidentiality, integrity, and availability of information, support information security within the organization, and to maintain a secure information technology (IT) environment. The College provides a safe and secure environment for the collection, storage, access and retrieval of information. Members of the College community are required to handle Humber College information assets responsibly within their respective roles and in accordance with this Policy.

Chief Information Officer

The Chief Information Officer ("CIO") oversees and is accountable for the development of Humber's Information Technology ("IT") Security Program. Responsibilities of the CIO include the following:

- Provide leadership and oversight on strategy, policy, and standards development
- Socialization of IT Security Program and related activities

Directory of IT Security

The Directory of IT Security is responsible for the planning, development and implementation of the IT Security Program. Responsibilities of the Director of IT Security include the following:

- Development and implementation of the IT Security Program including associated policy and standards.
- Development of IT Security Roadmap to achieve long range compliance goals.
- Track and measure the effectiveness of security controls, policy and standards.

Technology and Information Management Steering Committee (TIMS)

The Technology and Information Management Steering Committee ("TIMS") is a forum for consideration of Institution-wide computing strategy and initiatives. Specific oversight responsibilities related to the IT Security Policy include the following:

- Reviewing policy, standards and initiatives in support of the IT Security Policy.
- Identify the business impact of proposed strategy.
- Agreement on critical IT Services and information assets
- IT Security governance and deciding on risk appetite and ownership on IT Security

Executive Sponsors

Executive Sponsors are senior-level employees who have planning and policy responsibility and accountability for major administrative data systems. Executive Sponsors have overall accountability for the security of IT Systems in which they own, however they may delegate activities to other employees such as Data Stewards or Data Administrators, and both must act in response to defined requirements. Responsibility of Executive Sponsors related to the IT Security Policy include the following:

- Accountable for ensuring that systems are assessed for security requirements including those flowing from legislative and contractual obligations.
- Accountable for ensuring that systems are designed, configured, implemented, operated, maintained, upgraded and decommissioned in accordance with Humber's security standards.

- Accountable for ensuring that College systems under their purview have an appropriately assigned Data Stewards and Data Administrator.

Data Stewards

Data Stewards are appointed by Executive Sponsors to implement data governance, privacy and security management policies. Responsibilities of Data Stewards include the following:

- Authorize the use of systems within their functional areas and monitor this use to verify appropriate data access.
- Support access by providing appropriate documentation and training to support College system Clients.
- Responsible for safeguarding system from unauthorized access through established procedures and educational programs.

Data Administrators

Data Administrators are functional or technical users that have operational responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of associated computer hardware and software platforms. Some data administrators may work in an IT department outside of a functional unit but have responsibilities for implement the decisions of the data stewards. Responsibilities of Data Administrators include the following:

- Responsible for ensuring that systems are assessed for security requirements including those flowing from legislative and contractual obligations.
- Responsible for ensuring that systems are designed, configured, implemented, operated, maintained, upgraded and decommissioned in accordance with Humber’s security standards.
- Responsible for the classification of information under their purview in accordance with institutional data classification standards, accuracy, and access/use of information in their custody.
- Responsible for implementing the technical features of the assets under their administration in accordance with policy, guidelines, and other requirements as deemed necessary by Data Stewards.

Data Users

Data Users are individuals who make use of information while performing assigned duties or fulfilling authorized activities within the college. They are full time, permanent employees (e.g., faculty, administrators, and support staff), other employees such as contract, consultants, agents, students, volunteers and guests. Data Users are responsible for:

- Taking appropriate measures to prevent loss, damage, abuse, or unauthorized access to information assets under their control.
- Respecting the classification of information as established by the Data Stewards and Executive Sponsors.
- Complying with all the policy requirements defined in the security, privacy and data governance policies and supporting procedures, rules and guidelines.
- Responsible for technology asset(s) assigned to them. They must be able to determine the function and location of technology assets under their custodianship and must ensure that assets transferred from their custodianship are clearly assigned to the next custodian.

6. ENFORCEMENT

- Suspected violations of the IT Security Policy and its associated standards may be reported to the CIO.
- Pending an investigation, Humber reserves the right to immediately suspend a Client's access to any and all technical services.
- Suppliers and guests who violate the IT Security Policy and its associated standards may have their Humber contracts terminated and/or be refused all future entry to Humber campuses.
- Employees and students who violate the IT Security Policy and its associated standards may be subject to disciplinary action up to and including termination of employment or expulsion.
- Non-compliance with the Policy may result in the termination of access to Humber's Information systems and disciplinary action in the case of malicious intent.

7. COMPLIANCE

- The Information Security Team may conduct IT Security assessments, audits, and other reviews to assess compliance with this Policy and the Information Technology Security Standards.
- The Information Security Team may also engage external auditing and/or professional services to conduct tests that measure compliance or identify areas of risk, in accordance with these policies and standards.
- Humber's review of the IT Security Policy will be performed annually or when significant changes occur.

8. INFORMATION CLASSIFICATION

Humber's information systems must be protected and consistent with *The Freedom of Information and Protection of Privacy Act (*FIPPA*)* and other legislation that may apply. Please refer to the Data Governance Policy <link> and Access and Privacy Policy <link> for information on Information Protection and Classification. (Appendix C).

9. POLICY EXCEPTIONS

Exceptions to this policy and IT Security Standards must be submitted to and approved by the CIO or designate (see Appendix B). Questions about this Policy can be directed to the IT Security Manager.

APPENDICIES:

Appendix A: RACI MATRIX: Roles and Responsibilities

Roles	*Responsible (R): Who is assigned to do the work* *Accountable (A): Who makes the final decision and has ultimate ownership* *Consulted (C): Who is consulted before a decision or action is taken.* *Informed (I): Who must be informed when a decision or action takes place.*	*TIMS*	*CIO*	*Executive Sponsor*	*IT Security Director*	*Data Stewards*	*Data Administrators*	*Data Users*
Activities	*Reviewing institutional policy and standards of IT Security, IT Security governance and deciding on risk appetite and ownership*	R	R	I	A	I	I	I
	Provides leadership and oversight on strategy, policy, and standards development. Also provides socialization of IT Security Policy.	I	A	I	R	C,I	C, I	I
	Development and implementation of the IT Security Program, Policy, Standards and IT Security roadmap to achieve long range compliance goals.	I	A	C, I	R	I	C, I	I
	Track/measure the effectiveness of Policy and Standards	I	C,I	I	A,R	I	C,I	I
	Classifying information in accordance with policies and guidelines	I	C, I	A	C, I	R	C,I	I
	Ensuring systems are assessed for security requirements	I	C,I	A	C, I	C, I	R	I
	Ensuring system development and decommissioning adheres to Humber's security standards.	I	C,I	A	C, I	C, I	R	I
	Safeguarding system from unauthorized access through established procedures and educational programs	I	C,I	A	C, I	R	C,I	I
	Managing the function and location of technology assets under their custodianship	I	I	I	I	A	R	I
	Complying with all the security requirements defined in the policy and respecting the classification of information	R	R	R	A	R	R	R

HUMBER

Appendix B: Exception Request Form

For Information Security Office Use Only				
Exception number:	***Date Received:***	***Submitter:***	***Organization:***	***Relevant Standard:***

Confidential (when completed)
Submit completed form to (email)
Attach additional pages as needed

Information Security Office
205 Humber College Blvd
416-675-6622 (ext. 4424)

EXCEPTION REQUEST FORM

Requestor's Name: **Date:**

Requestor's Phone Number:

Requestor's Email Address:

1. Specific Standard/Policy for which an exception is being requested:

2. Specific device/application or service for which an exception is being requested:

3. Data classification category of associated device, application or services:

4. Type of data that will be affected, either directly or indirectly, by the exception:

5. Nature of non-compliance (i.e., specific deviation from the standard, policy.):

6. Why an exception is required, e.g., what business need or situation exists, what alternatives where considered, and why are they not appropriate:

7. Assessment of the potential risk posed by non-compliance, i.e., if the exception is granted:

8. Plan for managing or mitigating those risks e.g. compensating controls, alternative approaches:

9. Anticipated length of non-compliance:

10. Additional Information as needed, including any specific conditions or requirements for approval:

For Information Security Office Use Only				
Approved	***Denied***	***More information requested***	***Information Security Office Signature***	***Date***
Comments (including Risk Weighting):				

Appendix C: Classification of Institutional Data

	Restricted Data	Sensitive Data	Public Data
Institutional Impact	The negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is usually very high and may include legal, financial, and reputational consequences.	The negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is moderate to high.	Public data does not pose a risk in terms of confidentiality but its quality and integrity is important to the reputation of the institution.
Description	Access to restricted data must be controlled from creation to destruction and is granted only to those affiliated with the college who require the data to perform their job. Included in restricted data are those which fall under privacy legislation including FIPPA and PHIPA. Also included are data related to highly sensitive college business including that may be legal, proprietary and strategic.	Sensitive data are intended to be protected from broad consumption on account of business concerns, such as those related to competition and institutional strategic decision-making. Examples may include data related to budgeting, financial reports, facilities and human resource information.	Public data is typically highly aggregated data such as those reporting high level college enrolments and other publicly reported metrics
Access	Access to these data occur only when it is in accordance with Humber's legitimate business purposes and when legislation permits. Requests for access should be directed to the Executive Sponsor or relevant Data Steward.	Access to these institutional data may be authorized by the Data Steward to groups or individuals based on their job classification or role. Authorized personnel may be given access to systems but typically to subsections of the data (e.g., as reports or dashboards) to prevent access to more sensitive data that is not required for business purposes.	Access to these data may be granted to any requester and will typically be through public websites or through requests to Data Stewards or Data Administrators in specific departments, such as Institutional Planning and Analysis or through the Communications departments.

Related Policies:

Access and Privacy Policy
Accessible Use Policy
Data Governance Policy

References:

Freedom of Information and Protection of Privacy Act (Ontario)

Personal Health Information Protection Act (Ontario)