Information Security Policy

Effective Date	Responsible Officer	Responsible Office	This Policy Applies to:
11/19/2020	Vice President of Technology & Chief Information Officer	Division of Technology Services	All University departments and all faculty, staff, students, contractors, student employees, and anyone with access to University information technology resources.

1. PURPOSE

Wentworth Institute of Technology ("the University") has adopted the following Information Security Policy ("Policy") as an umbrella safeguard measure to reduce risks to the confidentiality, integrity, and availability of information technology resources ("ITRs").

2. SCOPE

This policy provides the foundation for the management of information security at the University and is the master policy document of the information security program.

3. POLICY STATEMENT

A structured Information Security Program shall be sanctioned by the Chief Information Officer and maintained by the Information Security Officer (ISO) to sufficiently mitigate risks to the confidentiality, integrity, and availability of University systems and data in electronic form. This policy and the University's supporting policies, operational plans, written information security program (WISP), guidelines, standards, and procedures are the documented elements of the program that facilitate its execution and maintenance. Policies in scope for the program will be reviewed on a recurring basis by the policy owner.

All systems shall be secured in a manner that reasonably and appropriately mitigates risks to a.) the highest level of data classification of information stored, processed, or transmitted on it and b.) the system's overall business criticality. Similarly, all information in electronic form shall be handled in a manner appropriate for its data classification level as determined by the associated University data custodian.

4. DEFINITIONS

Third-party	Any third-party hired or contracted by the University to provide services and who also stores, processes or transmits Institutional Data or uses Systems as part of their duties or service delivery.
Data	Any data in the custody of the University, regardless of whether it is owned, licensed, or only managed by the University.

Information Security Program	The design, execution, and maintenance of the processes, plans, policies, and procedures involved in lowering risks to Data and Systems by the ISO and other delegates of the CIO.
Information Technology Resource	Information technology resources ("ITRs") are Wentworth owned, leased, and/or managed information, technology, or IT services, which include but is not limited to computer accounts (email, network, system, application, et al), computers (desktops, laptops, workstations, servers, classroom A/V, and all mobile devices), printers and other peripherals, telephones and facsimile machines, electronic technology (i.e., computer programs, folders, and files), local and wide area networks, Internet access, digital storage media, and any information that resides on or traverses these resources
System	Any electronic technology that stores, processes, or transmits information on behalf of the University. Examples are servers, workstations, computer networks, mobile computers. and enterprise applications.
Written Information Security Program (WISP)	A document that describes in detail the elements of the information security program, such as governance aspects, risk management methodology, and the policies, plans, and procedures that support the program objectives.

5. RELATED DOCUMENTS

Document Name	Publisher[1]
Written Information Security Program	WIT
Information Technology Resource Acceptable Use Policy	WIT
Stewardship of Information Policy	WIT
Policy on Accessing University IT Resources from Personally-owned Computing Devices	WIT

6. ENFORCEMENT OF POLICY VIOLATIONS

Failure to comply with this policy may result in one or more of the following:

- Temporary suspension or permanent loss of the violator's privileges with respect to access to Institutional Data and/or University-owned Information Systems.
- Disciplinary action up to and/or including termination of employment.
- Civil or criminal penalties as provided by law.

7. EXCEPTIONS

Exceptions to this policy must receive written approval from the Information Security Officer, under the guidance of the CIO, and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

8. REVIEW AND REVISION HISTORY

[1] For documents originating within WIT, such as policies or procedures, specify "WIT". For other relevant third-party documents, such as external standards to which WIT subscribes, list the name of the organization that publishes the document.

Policies must be reviewed periodically by the Responsible Officer or delegate. If a policy has been revised, then it must have all necessary approvals before being published. In the last column, indicate whether the activity was a review or revision; if a revision, summarize the changes.

Date	Name and Title	Annual Review or Revision Summary
6/7/22	Bryce Cunningham, Information Security Officeer	Annual review