# Information Security Policy

**Category:** Operations

**Approval:** PVP

**Responsibility:** Associate Vice President, IT

**Date:** April 5, 2018; revised March 3, 2025

Definitions:

## Data or Privacy Breach

An incident in which internal, confidential, or restricted data has potentially been viewed, stolen, or used, or altered by an individual unauthorized to do so.

## Compromised Data

The data exposed in a data or privacy breach.

## Public or Unrestricted Data

Public data refers to information that is openly available to anyone, typically without restrictions or limitations on access. This type of data is often sourced from publicly accessible government agencies, academic institutions, research organizations or publicly available datasets. Public data is freely accessible and can be used by individuals, businesses, researchers, and policymakers for various purposes such as analysis, research, decision-making, and innovation.

## Internal Data

Internal data refers to information and resources that are generated, collected, or utilized within the institution for administrative, academic, or operational purposes. This includes data that does not contain identifiable information related to alumni, student enrollment, academic records, course schedules, research projects, campus facilities, financial transactions, and institutional policies and procedures. Examples of internal data may include student enrollment numbers, faculty teaching assignments, budget allocations, and administrative reports.

## Confidential Data

Confidential data refers to information that is considered sensitive and requires protection from unauthorized access, use, or disclosure due to privacy, security, or legal considerations. This may include personally identifiable information (PII) of students and alumni, faculty, and staff (such as social security numbers, student ID), financial data (such as bank account details or credit card numbers, donation records), academic records, and research data with privacy or intellectual property concerns. Confidential data may also encompass institutional strategies, policies, and plans that are not meant to be publicly disclosed.

Access to confidential data is restricted to individuals with a legitimate need to know, such as university administrators, academic advisors, human resources staff, and researchers working on relevant projects.

### Restricted Data

Restricted data refers to a subset of confidential data that is subject to additional access controls or limitations beyond standard confidentiality requirements. This may include information that poses significant risks if accessed or disclosed improperly, such as classified research data, proprietary information, trade secrets, or data subject to specific regulatory requirements, for example, health information.

Access to restricted data is tightly controlled and may be limited to a select group of authorized individuals or roles within the university.

### Personally Identifiable Information (PII)

Information relating to an individual that reasonably identifies the individual, either directly or indirectly. All PII that is in the custody of the university is classified as confidential or restricted data and should be made available on a least-privilege basis.

### Financial Data

Data about an individual's or an organization's financial matters, such as income, expenses, banking, and credit information.

### Research Data

Data collected, obtained, and used during the course of research. Includes original data, previously existing data sets, as well as the analysis, results, or dissemination resulting from the research process.

### Electronic Data

Data that are stored, transmitted or read in an electronic format such as a file on a drive or device, information in a database, or unstructured formats such as email.

### Cloud Service

Refers to remotely hosted computing resources, applications, and data storage which is operated by a third party and is not directly controlled by the University.

### Data subject

The person, object, or entity that the university collects data about.

### Data Owner

The managerial head of a unit or department with custodial responsibility or accountability for the maintenance and integrity of a type of university data on behalf of a data subject. For example, the Registrar as the data owner of student record data or the AVP-Finance as the data owner of university financial data.

### Data User

An individual authorized by a data owner to access and maintain some university data.

## Storing Electronic Data

- Refers to the practice of placing a non-transient copy of electronic data on any device or cloud service, including:
    - Servers and applications managed by Trent IT and in Trent data centres;
    - Computer or laptop hard drives;
    - Mobile devices such as smartphones, tablets, and wearable devices;
    - Portable storage media such as USB memory cards, external hard drives, SD cards, CD-ROM, DVD, magnetic tape, floppy disks, etc.;
    - Cloud services
    - Email;
    - Any other electronic device that can store information.

## Transmitting Electronic Data

The process of sending data over any communication medium to one or more computing, network, communication, or electronic devices. Remotely accessing data is also a form of transmission.

## Encryption

The act of transforming information into an unintelligible format that can only be accessed using an authorized key, password, or other security token.

## Password Vault

A software application designed to store login credentials in an encrypted database.

## Trent Credentials

A username and password issued and managed by the University IT department and used to access the University's IT resources.

## Multi Factor Authentication (MFA)

An authentication system which combines a password with a second credential, such as a smartphone app, to better secure the login process and provide additional protection.

## Virtual Private Network (VPN)

An encrypted connection between a computer and the University network that securely crosses the internet.

## Data Loss Prevention

A series of tools that can be used to automatically protect and restrict the storage and transmission of confidential and restricted data.

## Purpose/Reason for Policy:

In conjunction with the principles outlined in the Trent University Policy on the Protection of Personal Information, the purpose of Trent University's Policy on Information Security (the Policy) is to establish a framework for classifying and handling electronic data which will;

- Ensure the University's statutory, regulatory, legal, contractual and privacy obligations with respect to privacy and data security are met, and;

- Ensure the University's proprietary data and information is kept confidential to the institution as required;

## Scope of this Policy:

This Policy applies to all administrators, faculty, staff, volunteers, authorized third party agents, and students employed, or contracted by, Trent University (the University), and its affiliates, who, as part of their role and responsibilities, may create, use, process, store, transfer, administer, and/or destroy data electronically.

The Policy applies to all electronic data in which the University has a legal interest or ownership right, regardless of where such data are stored.

Where legal, contractual, or funding agency obligations impose an alternate requirement for data protection, the Associate Vice President, Information Technology (AVP-IT) will determine if that alternate meets the requirements of this Policy. If the alternate requirement is more stringent, then it shall supersede only the directly relevant section of this Policy and with regard only to sensitive information falling under the purview of that third-party entity.

## Policy Statement:

Administrators, faculty, staff, volunteers, authorized third party agents, and students employed or contracted by, Trent University (the University), and its affiliates must use care when handling sensitive electronic information and must abide by the provisions of this policy and the accompanying data classification and handling guideline when working with university data throughout its lifecycle.

The data classification and handling guideline contain examples of how data should be classified and protected. Federal and provincial legislation, as well as contractual obligations and agreements may also specify data elements that require protection from unauthorized creation, access, modification and/or deletion.

The IT department will provide the necessary technology support for the implementation of this Policy. Information about these services can be found on the IT website at www.trentu.ca/it. The IT department may also deploy automated tools intended to detect and/or prevent data breaches or violations of this policy in real time.

While the data classification and handling guidelines should be viewed as a supplement to this policy to enhance understanding, specific requirements are listed as follows:

| Storage of Data | | | |
|---|---|---|---|
| Unrestricted | Internal | Confidential | Restricted |
| No restrictions | Should only be stored on:<br><br>All locations for confidential and restricted data OR: On computers and laptops supported by | Should only be stored on:<br>• Central servers and cloud services maintained by Trent IT<br>• On computers and laptops supported by Trent IT that have been encrypted using IT-approved full-disk encryption software | |

| | | |
|---|---|---|
| | Trent IT that have been encrypted using IT-approved full-disk encryption software | • On an encrypted mobile device with applications supported by Trent IT<br>• With research or business partners, if a formal agreement is in place to ensure that the partner will comply with the requirements of this policy.<br>• Any other location approved by IT |

Confidential and restricted information may **NOT** be stored:

- on unencrypted computers, laptops, devices, or portable storage;
- on computers not supported and managed by Trent IT;
- with cloud storage services where credentials are not managed by Trent IT; and
- in any other location not approved by IT.

## Transmission

| Transmission of data | | | |
|---|---|---|---|
| Unrestricted | Internal | Confidential | Restricted |
| No restrictions | Should only be transmitted using:<br>• The wired campus networks<br>• The eduroam wireless network<br>• Accessing the University network via VPN<br>• The Secure Shell (SSH) protocol<br>• Any chat or messaging program approved by IT<br>• Secure HTTP (HTTPS), when the web site certificate is considered valid by the browser<br>• Trent provided e-mail utilizing data loss prevention controls<br>• Any other method approved by Trent IT | | |

The following communication channels are considered to be **NOT** secure and should not be used for the transmission of data other than unrestricted data;

- Remote access solutions or methods not approved by IT;
- unencrypted protocols such as FTP, Telnet, or HTTP;
- any open wireless network or public hotspot;
- any messaging/chat program, such as iMessage, WhatsApp, etc., not approved by IT;
- SMS text messaging;
- social media; and
- Public email accounts.

## Third Party Access:

When confidential and restricted information is stored by, accessed by, or transmitted between the University and third parties (e.g, contractors, business partners, research collaborators), a formal agreement must be in place ensuring the third party's compliance

with the Policy and any accompanying guidelines. Additionally, contractors must undergo a Security Impact Assessment completed by IT.

### Disposal of Confidential Information

Any media which has been used to store highly sensitive or sensitive electronic information must be either physically destroyed or brought to IT for secure disposal.

### Protecting Passwords

To maintain the availability of encrypted data, passwords should be stored in a password vault, using MFA, so that they can be recovered in the event that a password is lost. This is particularly important for individually encrypted files, where there is no password reset option available.

### Exceptions

Requests for exceptions to the Policy must be submitted to the Associate Vice President, IT.

### Non-Compliance

Departments and users who act in good faith and execute their responsibility with a reasonable standard of care shall not be subject to disciplinary action in the event of a data security breach.

Breaches arising from intentional disregard of this policy will be subject to sanctions determined by the AVP-IT up to and including the suspension of computing privileges and account access. For unionized employees, any disciplinary action resulting from intentional violation of this policy will be consistent with collective agreement provisions and will be imposed in accordance with procedural requirements of the collective agreement and all rights thereunder shall be preserved.

### Reporting

In the event of an actual or suspected data breach, the user must inform both IT and the University's Access and Privacy Office. If the breach involved research data, the Office of Research must also be informed.

In addition to the above, if the breach involved the physical theft of a device, the theft must be reported to Campus Security.

## Contact Officer:

Associate Vice President, IT

## Date for Next Review:

February 2027

## Related Policies, Procedures and Guidelines:

- Data Classification and Handling Guideline
- Computing Resources Acceptable Use Policy
- Network Connection Policy
- Computing Privileges Policy

## Information Access Policy Policies Superseded by this Policy:

- Guidelines for Use of Information Technology