Handling Sensitive Information Policy

Category: Operations

Approval: PVP

Responsibility: Associate Vice President, IT

Date: April 5th, 2018

Definitions:

Data or Privacy Breach
An incident in which sensitive or highly sensitive 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.

Sensitive Data
Data, information, or intellectual property in which the University has a legal interest or ownership right and is intended for only limited dissemination. Such materials, if compromised, could be expected to cause minor, short-term harm or embarrassment to the institution and/or specific individuals.

Highly Sensitive Data
Data, Information, or intellectual property in which the University has a legal interest or ownership right and is intended for only limited dissemination. Such materials, if compromised, could cause significant and/or long-term harm to the University. The major difference between Highly Sensitive Data and Sensitive Data is the likelihood, duration, and the level of harm potentially incurred by a breach.

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 highly sensitive information.

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.

Storing Electronic Data

Refers to the practice of placing a non-transient copy of electronic data on any device or cloud service, including:

- Servers 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.

Two Factor Authentication (2FA)

An authentication system which combines a password with a second credential, such as a smartphone app, SMS message, or physical device.

Virtual Private Network (VPN)

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

Documents Rights Management

Documents Rights Management is a subset of Digital Rights Management technologies that protect sensitive information from unauthorized access. These technologies ensure that certain policies can be applied to documents and e-mail, including; controlling access, printing, and distribution beyond the intended recipients.

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 Handling Sensitive Electronic Information (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 following as related to the storage, transmission, access, and disposal of electronic data.

Appendix A provides some common examples of sensitive and highly sensitive information. 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 security website found at URL: www.trentu.ca/it/security. The IT department may also deploy automated scanning tools intended to detect and/or prevent data breaches in real time.

Storage:

Highly Sensitive Information

Highly sensitive electronic information may only be stored;

- on central servers which are managed directly by the Trent University Information Technology Department (IT) (H: and S: drives, Blackboard, Colleague, etc.);
- on computers and laptops that have been encrypted using IT-approved full-disk encryption software;
- on an encrypted mobile device;
- on USB memory sticks or portable hard drives that have been encrypted using IT-approved full-disk encryption software or built-in encryption compliant with the FIPS 140-2 standard;
- with IT-approved cloud services which require Trent credentials to access;
- 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, and;

- in any other location approved by IT

Highly sensitive electronic information may not be stored;

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

Please note that accessing email from a mobile device will sync a portion of your mail to that device. If you expect to send or receive sensitive or highly sensitive information via email, you must abide by the above as related to storage.

Sensitive Information

All rules for the storage of highly sensitive information also apply to sensitive information, with the exception that sensitive information may also be stored encrypted on an unencrypted device or public cloud storage service.

Transmission

In general, transmission and remote access of both Highly Sensitive and Sensitive Electronic Information is permitted over a secure communication channel, when the source and destination are both approved for storage of the data.

The following communication channels are considered secure;

- the wired campus network;
- the eduroam wireless network;
- accessing the University network via VPN;
- the Secure Shell (SSH) protocol;
- any chat or messaging program approved by IT, and;
- secure HTTP (HTTPS), when the web site certificate is considered valid by the browser;
- Trent provided e-mail utilizing Documents Rights Management.

The following communication channels are considered to be not secure;

- logmein, teamviewer, or any other remote desktop access method not approved by IT;
- unencrypted protocols such as FTP, Telnet, or HTTP;
- any open wireless network or public hotspot, including the Trent guest network;
- any messaging/chat program, such as iMessage, WhatsApp, etc., not approved by IT;
- SMS text messaging;
- social media, and;
- Public email accounts

When no secure transmission protocol is available, an insecure method may be used to transmit encrypted files containing Sensitive Data, but not Highly Sensitive Data.

Third Party Access:

When sensitive or highly sensitive data 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. 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 2FA, 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:
April, 2021

Related Policies, Procedures & Guidelines
a) Computing Resources Acceptable Use Policy
b) Network Connection Policy
c) Computing Privileges Policy
d) Information Access Policy

Policies Superseded by This Policy:
a) Guidelines for Use of Information Technology

Appendix A – Data Classification
The following data classifications are not exhaustive. The Office of Research is the authoritative source for the classification of research data, and the Access and Privacy Office is the authoritative source for the classification of all other data.

Sensitive Information

Data, information, or intellectual property in which the University has a legal interest or ownership right and is intended for only limited dissemination.

Examples may include, but are not limited to;

- draft planning documents;
- internal websites;
- meeting minutes before their approval;
- unreleased public announcements, and;
- procurement process documents (pre-award)

Highly Sensitive Information

Data, information, or intellectual property in which the University has a legal interest or ownership right, and which, if compromised, could cause significant harm to the University.

Examples may include, but are not limited to;

- research data;
- personally identifiable information
- financial information and contracts;
- trade secrets and patent applications;
- account passwords or encryption keys used to protect access to University data, and;
- data from a third party when the University has agreed to keep such material confidential

Personally Identifiable Information

Information relating to an individual that reasonably identifies the individual. Personally identifiable information is further defined by both federal and provincial legislation.

Examples may include, but are not limited to;

- the individual's name if it appears with other private information relating to the individual or where disclosure of the name would reveal other private information about the individual;
- any identifying number, symbol or other particular assigned to the individual;
- the address, telephone number, email address(es), personal electronic identity(ies), or biometric identifiers of the individual;
- information relating to the race, national or ethnic origin, religion, age, sex, sexual orientation, gender identity, or marital or family status of the individual;
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual;
- information relating to financial transactions in which the individual has been involved;
- student grades or disciplinary information;
- salary or employee performance information, and;
- correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence.