Data Classification and Handling Guidelines

Associated Policy: Information Security Policy

Approval:PVP

Sponsor: Associate Vice President, IT

Date Initially Approved: TBC Introduction

This guideline is designed to augment the Information Security policy by providing additional guidance, examples, and specific instructions for the handling of sensitive data at Trent University.

Sensitive data can be stored, transmitted, and controlled through many modes and methods. The Information Security policy is designed to broadly define how data should be handled, stored, and cared for at the university. This document is a supplement to that policy, providing additional context, advice, and practices to further secure sensitive data.

Definitions

**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 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, faculty, and staff (such as social security numbers, student ID), financial data (such as bank account details or credit card numbers), 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.

How to use

The first pages of this document assist with the classification of sensitive information by providing examples and risk levels to accompany each of the information classification types defined in the policy. Begin by establishing the classification level of the data that is being stored, transmitted, or protected.

After classification has been established, the subsequent sections of the document provide information for how the data should be transmitted, stored, and handled. Although this listing is not exhaustive or comprehensive, it is designed to provide context on how sensitive data should be handled.

Information Classification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Classifications | Unrestricted | Internal | Confidential | Restricted |
| Examples of Information Types | * Brochures and marketing material * Trent University website * General and course/program information * Staff and faculty contact information. * Policies * Academic calendars | * General correspondence * Staff and employee newsletters * Inter-office memorandums * Non-personally identifiable information * Internal processes and procedure outlines * Purchasing information * Vendor contacts * Purchase requisitions | * Personally identifiable   information (PII)   * Credit card information * Financial documents * Faculty and staff records * Student records * Contractual agreements * Intellectual property * Cheques * Passwords | * Large amounts of personally identifiable   information (PII)   * Strategic organizational plans / financial information * In-camera senate and board meetings (closed portions) * Sensitive meeting minutes * Personal Health Information (PHI) |
| Information Classifications | Unrestricted | Internal | Confidential | Restricted |
| Examples of Risk Impacts | * Little or no impact * Minimal inconvenience if not available * If modified or destroyed would not result in legal liability | * Disruption to business if not available * Low degree of risk if corrupted or modified * Low risk to safety, minimum impact on workload * Minimal potential liability * Minimal financial consequence | * Disruption to business if not available * moderate - high degree of risk if corrupted or modified * Moderate - high risk to safety, minimum impact on workload * Moderate -high potential liability * Moderate -high financial consequence | * Significant loss of reputation * Serious impact and disadvantage to funding * Significant potential liability (civil & criminal) * Significant financial consequences or loss of funding * Significant impact to strategic planning activities |

Information Handling Guidance

*Transmission*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Classifications | Unrestricted | Internal | Confidential | Restricted |
| Conversations and meetings | * No special precautions required * Ensure that you are not overheard | | Private setting / lowered voices | Enclosed meeting space |
| Telephone | * Avoid proximity to unauthorized listeners * Speakerphone only in enclosed meeting spaces | |
| Voicemail |
| Inter-office mail | * No special precautions required | | * Sealed envelope * Market private and confidential | * Sealed envelope * Market private and restricted * Notify recipient in advance |
| External mail |
| Email – internal | * Use of e-mail strongly discouraged, unless encrypted. * Credit card information (PCI) strictly prohibited | * Use of e-mail strongly discouraged. |
| Email – external |
| Website and social media | * Content must be authorized by head of department or faculty or their assigned delegate. * All websites must be appropriately secured to allow only authorized content modification and administration | | * Strictly prohibited | |
| myTrent portal | * Content must be authorized by head of department or their assigned delegate. | | * Access to confidential information must be restricted to authorized individuals only. | |
| Electronic file transfer | No special precautions required | No special precautions required | Prohibited unless encrypted (i.e. SSL, SFTP, or VPN) | Prohibited unless approved by Trent IT. |
| Fax | Verify fax number prior to transmission | | Strictly prohibited | |

*Storage*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Classifications | Unrestricted | Internal | Confidential | Restricted |
| Free or personal storage services (Dropbox, Google Drive) | No special precautions required | Strictly prohibited | | |
| Personally owned computing devices | No special precautions required | Storage on devices with full-disk encryption. | Strictly prohibited | |
| Servers operated by 3rd parties or co-located IT services. | No special precautions required | | Strictly prohibited unless approved by Trent IT with appropriate, managed intrusion prevention and response technologies. | Strictly prohibited |
| Trent IT provided services including cloud services and IT provided devices | No special precautions required | | Access to confidential restricted information must be restricted to authorized individuals only. | |

*Destruction*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Classifications | Unrestricted | Internal | Confidential | Restricted |
| Printed materials | No special precautions required | No special precautions required | Must be shredded and securely disposed of. | |
| Digital storage devices (hard drives, disks) | No special precautions required | Deleted by computer operating system | Physical destruction as provided by Trent IT. | |

*Physical Security*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Classifications | Unrestricted | Internal | Confidential | Restricted |
| Computers and laptops | No special precautions required | * Devices must be supported by Trent IT * Applications and Operating System should be set to automatically update * Password protected screensavers should be used whenever left unattended * Computers must be appropriately secured when left unattended | * Devices must be managed by Trent IT * Device must include appropriate anti-malware and threat prevention, as approved or provided by Trent IT. * Applications and Operating System should be set to automatically update * Password protected screensavers should be used whenever left unattended * Computers must be appropriately secured when left unattended | |
| Monitors | No special precautions required | Positioned or shielded to prevent viewing by those not authorized | | |
| Printing | No special precautions required | | * Print only when absolutely necessary. * Unattended printing is not permitted. | |
| Office access | Work areas must be secured from public access while unattended | | * Access to areas containing sensitive information should be physically secured. * Confidential and restricted information must be locked when left in an unattended room or filing cabinet. | |
| Mobile devices – tablets and mobile phones | No special precautions required | Pin or password protection must be used | * Pin or password protection must be used. * Encryption of device contents | |

*Access Control*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Classifications | Unrestricted | Internal | Confidential | Restricted |
| Access control | Available to the public | Generally available to all staff and faculty on a need-to-know basis. | Must have a business need to know as determined by the data owner / custodian. | Must have written approval of the data owner. |

*Audit*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Classifications | Unrestricted | Internal | Confidential | Restricted |
| Audit | None | None | Access should be audited as determined by the data owner / custodian | |

### Date for Next Review:

February 2027