Version 1.8

TRU Information Classification Standard

September 2016

Governing Laws and Regulations		**FIPPA**: 30, 30.1		**PCI DSS**: 3.1, 3.2c, 3.3, 4.1, 4.1a, 4.2, 4.2b	
CLASS	**DEFINTION**	**ACCESS RESTRICTIONS**	**TRANSMISSION**	**STORAGE**	**DISPOSAL**
Public	Information deemed to be public by legislation or policy. Information in the public domain. Examples include annual reports, public announcements, the telephone directory, and specific categories of employee and student information including, employee business contact information and student's record of graduation. **Sensitivity**: Low	No restrictions on access.	No special handling required.	No special safeguards.	Can be recycled.
Internal Use	Information not approved for general circulation outside Thompson Rivers University. Loss would inconvenience the organization or management; disclosure is unlikely to result in financial loss or serious damage to credibility. Examples include internal memos sent to faculty/staff, minutes of meetings, internal project reports, unit budgets, accounting information. **Sensitivity**: Low/Medium	Access is limited to employees and other authorized users and must be revoke immediately on termination.	No special handling required but encryption is strongly recommended on public networks.	Stored within a controlled access system (e.g. password protected file or file system or locked file cabinet).	Shredded, erased.
Confidential	Information that is available only to authorized persons. Loss could seriously impede the organization's operations; disclosure could have a significant financial impact or cause damage to the organization's reputation. Examples include information protected by legal privilege, all Personal Information (PI) governed by the BC FIPPA, specific categories of employee and student information such as legal suits, medical/health information, appeals, grievances, bank routing information, credit card information, as well as clinical patient data and Requests for Proposals during a purchasing process. **Sensitivity**: High	Access is limited to authorized users with a demonstrated need to know and must be revoke immediately on termination or on leaving a custodial unit. Access must be from within Canada unless temporarily traveling or an exception is granted by the CIO. Remote Access: authorized persons require; automatic disconnect of session after 15 minutes of idle time and may not copy, move, or store credit card or banking data to remote devices. Note: The Credit Card PAN must be masked with the exception of the first and last four digits and only those with a business need to know may access the full PAN.	Encryption required for external networks. Encryption optional on internal networks. Hard copies must use secure methods for external transportation and be clearly marked as confidential. Note: Use of 3rd party services must comply with the Cloud Security Standard. Note: Credit Card Information must always use strong cryptography and security controls and may not be sent or accepted by email or other end user messaging technologies.	Stored within a controlled access system within locations defined by the CIO and AVP ITS (e.g. password protected file, file system or locked file cabinet or storage container). For any portable medium such as USB drives, notebooks, tablets, and SmartPhones - Encryption required. PI must be stored in Canada or comply with the Cloud Security Standard. Note: Credit Card Information must always be encrypted and should not be stored. Prior to disposal, hardcopy information must be stored in secure containers.	Cross cut shredded, pulped, degaussed (removal of magnetic information), or Securely Erased to render any information unrecoverable. Note: Credit Card Sensitive Authentication Data must be deleted upon completion of authentication and Personal Account Numbers must be securely deleted/destroyed as soon as business requirements have been met.

Note: TRU's Records Retention Policy must be considered for all class types.