Cloud Security Standard – Adopted by the TRU Information Security Committee October 25, 2012

This standard is intended to address the information security requirements for using Cloud Services for the storage, processing, or transmission of University information. Cloud Services include any electronic service hosted outside of the University network. e.g. Gmail, Youtube, Dropbox, Google docs, etc.

Cloud Security Standard

The use of any cloud service for the storage, processing, or transmission of **personal information** is prohibited unless authorized by a senior executive. The use of any cloud service for the storage, processing, or transmission of any other confidential university data is prohibited unless a contract is in place which has undergone review by the University's General Counsel and the TRU Information Security Committee. This review will ensure compliance with university policy, provincial and federal law, and contractual obligations. In cases where large volumes of data may be stored, processed, or transmitted using cloud services, a Privacy Impact Assessment for personal identifiable information or a risk assessment for other data may be required to be performed.

A review of cloud services contracts will ensure:	**Responsibility**
1. that the university is not subjected to unreasonable risks from the misuse of information	Department
2. datacenters are located within Canada	Department
3. confidential data is stored and transmitted in an encrypted format	Department
4. confidential data is disposed of appropriately	Department
5. cloud vendors are able to certify their security program by independent audits acceptable to TRU	Department
6. cloud service providers enforce adequate hiring, oversight of staff, and access controls	Department
7. providers can guarantee complete data segregation of university information for secure multi-tenancy	Department
8. the hosting provider has the ability to do a complete restoration in the event of a disaster	Department
9. any vendor usage of university information is determined	Department
10. companies working with the vendor meet clear security guidelines	Department & ISO
11. compliance with university policy, law, and contractual obligations	Department & Legal
12. the provider is meeting regulatory requirements	Department & Legal
13. the vendor commits to following specific privacy requirements	Department & Legal
14. the University retains ownership and is accountable for its own data	Department & Legal
15. backup data belongs to TRU	Department & Legal
16. vendor storage and use of their logs are managed appropriately	ISO
17. the portability of data to avoid lock-in or potential loss if the business fails	ISO
18. indemnification policies are in place in the event of a regulatory issue	Legal
19. software escrow is included in any contract for cloud services	Legal