TRU Account Management Standard

Ratified by the TRU Information Security Committee on September 27, 2016

Purpose

The quality and integrity of Thompson Rivers University's information system accounts are the only legitimate method by which Thompson Rivers University information systems may be accessed. Without active account management, the potential exists that legitimate users can use these accounts for illegitimate purposes. Additionally, the potential exists that these accounts can be usurped and used illegitimately to access Thompson Rivers University's information systems.

Scope

The Account Management Policy applies to all employees of Thompson Rivers University, including all temporary or contract workers. Specifically, it includes:

- Servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, wireless access points and other devices that provide network capabilities.
- Firewalls, Intrusion Detection/Prevention, and other devices that provide dedicated security capabilities.

Governing Laws, Regulations & Standards

Guidance	Section
Payment Card Industry Data Security Standard (PCI DSS) v3.2	2.1, 2.1.1, 8.1, 8.2,
BC Freedom of Information and Protection of Privacy Act	30, 30.1

Standards Statements

1. All information system accounts will be actively managed by appropriate administrative staff. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
2. Information system accounts are to be constructed such that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with that account. Further, accounts shall be created such that no one account can authorize, perform, review, and audit a single financial transaction to eliminate conflicts of interest.
3. Information system accounts are to be reviewed to identify accounts with inappropriate privileges (either too high or too low) on an annual basis. Should information system accounts be discovered with inappropriate privileges, those privileges will be manually reset to the established level.
4. Information system accounts are to be reviewed to identify inactive accounts. Should information system accounts that are associated with an employee or third party be discovered that have been inactive for one year the owners of the account will be notified of pending disablement. Should the account continue to remain inactive for one year, it will be manually disabled.
5. Vendor-supplied defaults are always changed and unnecessary accounts are eliminated before installing a system on the network.
6. Wireless vendor defaults are changed at installation or anytime anyone with knowledge of them leaves the company including:
    a. Encryption keys.
    b. Default SNMP community strings
    c. Default passwords/passphrases on access points.