Thompson Rivers University - Access Control Standard

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

Purpose

The purpose of this standard is to ensure users have appropriate access levels which specifically authorize them to access information on Thompson Rivers University's systems and applications.

Scope

This Standard applies to all university processes and data, information systems and components, personnel, and physical areas of Thompson Rivers University.

Governing Laws & Regulations & Standards

Guidance	Section
PCI DSS v 3.2	7.1, 8.1.1, 8.1.3, 8.1.5, 8.1.6, 8.1.8, 8.7.b, 9.1.1, 9.1.2, 12.3.6,12.3.9
BC FIPPA	30, 30.1

Standard Statements

- This standard will be reviewed annually by the TRU Information Security Committee.
- Thompson Rivers University will employ role-based access and will follow the principle of least privilege.
- Users will only receive access to networks and systems specifically authorized to them.
- All users with access to any Payment Card Industry Card Data Environment (PCI CDE) will be assigned a unique UserID. Generic accounts must not be used to access systems in these environments.
- All accounts used to access any PCI CDE will be deactivated after 90 days of inactivity.
- All third party vendor accounts, if applicable, will be disabled when not in use.
- All sessions within the PCI CDE will be disabled after 15 minutes of idle time.
- All direct access to databases containing PCI Card Holder Data (CHD) will be restricted to database administrators.
- Any third-party remote access to the PCI CDE will be enabled only when needed and deactivated immediately after use.

User Access Management

- TRU's Applications and Systems Access Request (ASAR) process must be used for user registration and de-registration processes to allow assignment of rights.
- Privileged access rights will be allocated using the above process with all access being approved by Data Owners. The usage of privileged accounts will be monitored by the TRU Information Security Office.
- In the PCI CDE:
    - direct access to or queries of databases must be restricted to database administrators.
    - all user access to, user queries of, and user actions on (for example, move, copy, delete), databases must be through programmatic methods only (for example, through stored procedures).
    - application IDs must only be able to be used by the applications (and not by individual users or other processes).
- Passwords will be forced to meet the TRU Password Standard on first login.
- Data owners or their delegates, must conduct annual reviews of users' access rights and use of accounts.
- With the exception of retirees access to email per the Emeritus/Emerita Designation Policy (BRD 15-3), upon termination of employment, an employee's or external party's user access rights will be revoked.
    - If there is a change to a contract or agreement, then the access will be adjusted appropriately.
    - Thompson Rivers University will employ automated processes to disable temporary contractor access on the VPN and manual processes for employee termination within 48 hours of notification to Information Technology Services.

System and Application Access Control

- All access to systems and applications will be restricted with a secure log-on process.
    - A limit of 10 successive incorrect logons will be enforced and an automatic account lock will be enabled for end user systems.

    - All systems in a PCI DSS Card Data Environment will be limited to 6 successive incorrect login attempts before the account is locked.
    - Time and date of logons and account changes will be recorded and monitored.
- Network and information systems sessions will remain locked until the user reestablishes access through an established authentication procedure.
- Password management systems will be interactive and mandate strong passwords.
- Thompson Rivers University's will control the flow of information between interconnected systems to ensure secure transfers through secure protocols where possible.
- Thompson Rivers University's will enact separation of duties to decrease the risk of abuse of privileges.
- Thompson Rivers University's will ensure the information sharing process follows appropriate access levels of sharing partners.
- Thompson Rivers University's will designate individuals allowed to post information on publicly available systems.

Physical and Logical Network Access

- Access to publicly accessible network jacks is controlled by physically disconnecting the jack for the network or disabling the port to which it is connected.
- Physical access to networking/communications hardware, gateways, and telecommunication lines is restricted using locked communications closets.
- Access to wireless access points is restricted by placement in inaccessible locations
- Access to handheld devices is restricted through placement in areas that are continuously monitored by staff.
- Taking into consideration the above controls acceptable network locations are determined by the Manager responsible for Network Services.