Thompson Rivers University - System Configuration Standard

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

Purpose

The quality and integrity of Thompson Rivers University standardized configuration settings allow information systems and information system components to be consistently deployed in an efficient and secure manner and assures compliance with Payment Card Industry Data Security Standards (PCI-DSS) v 3.2. Without standardized configuration settings, the potential exists that information systems may be deployed that fail to meet the security requirements of Thompson Rivers University, or that compromise the security requirements of other information systems with which they interconnect.

Scope

This Systems Configuration Standard applies to all information systems and information system components of Thompson Rivers University. Specifically, it includes:

- Servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, multi-function devices (copier/printers/faxes) and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

Governing Laws & Regulations

Guidance	Section
BC Freedom of Information and Protection of Privacy Act	30, 30.1
Payment Card Industry Data Security Standard (PCI DSS) v3.2	2.2.b, 12.3.4

Standard Statements

1. Standardized configurations, or baselines, have been established and are maintained for all information systems. These baselines indicate the specifications of information system components (hardware, firmware, and software), and allow for accurately and readily determining the owner, contact information and the purpose of the device. These configuration standards will be updated whenever new vulnerabilities are discovered and the remediation requires a change to configurations.
2. A CMDB that includes information system components for central computing systems is maintained. The inventory is updated whenever a new information system or information system component is implemented, or when an old one is retired.
3. Separate systems are maintained that includes all desktop (SCCM) and MFD hardware and software.
4. A complete set of documentation is maintained for each information system. This documentation will include administrator and user guides for each information system component as well as guides to the functional properties of integrated security controls.
5. Networks will be configured to restrict information flow between information systems or components of information systems through the use of Access Control Lists. Further, wireless networks will be restricted and may only be used where documented authorization exists.
    a. There is a formal process for approving and testing all network connections and changes to the firewall and router configurations which is addressed in the firewall and router configuration standards? TBD
    b. Current up-to-date network diagrams and card holder data flow diagrams that document all connections between the cardholder data environment and other networks, including wireless networks are maintained by the ITS Technical Services Department.

c. Consistent with current network diagrams, firewalls are implemented at each Internet connection and between the demilitarized zone (DMZ) and the internal network zones.

d. A DMZ is implemented to limit inbound traffic to only IP Addresses and system components that provide authorized publicly accessible services, protocols, and ports.

e. Anti-spoofing measures are implemented to detect and block forged sourced IP addresses from entering the network.

f. Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized per “supporting procedure”. TBD

g. Only established connections are permitted into the network.

h. System components that store PCI cardholder data (such as a database) are placed in an internal network zone, and are segregated from the DMZ and other untrusted networks.

i. Methods are in place to prevent the disclosure of private IP addresses and routing information to the Internet.

j. Any disclosure of private IP addresses and routing information to external entities is authorized in “supporting procedure”. TBD

k. All vendor-supplied defaults are changed and unnecessary default accounts are eliminated

l. Only one primary function is implemented per server or virtual system to prevent functions that require different security levels from co-existing on the same server.

m. Additional security features for any required services, protocols or daemons are implemented that are considered to be insecure.

n. System security parameters are configured to prevent misuse.

o. All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers are removed.

p. Only necessary services, protocols, daemons, etc. are enabled as required for the function of the system; services and protocols not directly needed to perform the device’s specified function are disabled.

q. All enabled insecure services, daemons, or protocols are justified per documented configuration standards.

r. System administrators and/or personnel that configure system components are knowledgeable about common security parameter settings for those system components.

s. Common system security parameters settings are included in the system configuration standards.

t. Enabled functions are documented and they support secure configuration and only this documented functionality is present on system components.

Procedure 1

Create an inventory that is keyed by system:

- Catalog specifications of all systems and system components:
  - All components that form the system.
  - Physical specifications for all components.
  - Data that is stored in or used by the system.
  - System and data owners.
  - Physical location of all system components.
  - Indicators if components belong to multiple systems.
- Catalog configurations of all systems and system component software:
  - Software (operating system and application) version.

  - Software (operating system and application) patch level.
  - Accounts.
  - Permissions of each account.
- Include the following documentation:
  - Implementation documentation.
  - Configuration documentation.
  - Operations documentation.
  - Test and assessment documentation.

Procedure 2

Keep the inventory up to date to ensure that the information it contains is complete and accurate:

- Update the inventory when systems or system components are implemented.
- Update the inventory when systems or system components are modified.
- Update the inventory when configurations of systems or system components are modified.
- Update the inventory when systems or system components are removed or replaced.
- Update the inventory when system or system component documentation is modified.

Procedure 3

Configure systems to provide appropriate security by default:

- Configure systems to provide only those services required by the system, disabling all others.
- Configure system accounts per the Account Management Standard.
- Configure system passwords per the Password Standard.
- Perform all system operations per the separately defined standard (i.e. TRU Account Management Standard, TRU Access Control Standard, TRU Operations Security Standard, ITS Change Control Policy, etc.).