TRU Operations Security Standard

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

Purpose

The purpose of this standard is to ensure the secure operations of information processing facilities within and related to Thompson Rivers University.

Scope

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

Governing Laws, Regulations & Standards

Guidance	Section
Payment Card Industry Data Security Standard (PCI DSS) v3.2	1.4, 6.1, 6.2, 8.3, 9.1.1, 9.2, 9.4.1, 9.4.4, 9.9.a, 9.9.b, 11.1, 10.6.1, 10.7, 12.1, 12.3.6, 12.3.7, 12.5, 12.5.1, 12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5, 9.1.1
BC Freedom of Information and Protection of Privacy Act	30, 30.1

Standard Statements

Operational Responsibilities

- The role of Manager Information Security will be established to oversee day to day operations of the TRU Information Security Program under the supervision of the Associate Vice President, Digital Stategy and CIO with oversight by the TRU Information Security Committee.
- The Manager Information Security will be responsible for drafting and documenting information security policies, standards and procedure for review and ratification by the TRU Information Security Committee (ISC) or the responsible TRU governance body. Once ratified it is the responsibility of the Manager Information Security to ensure these documents are distributed to all relevant personnel.

Operational Procedures

System Configuration

- A standardized configuration, or baseline, will be established and maintained for all information systems. These baselines will indicate the specifications of information system components (hardware, firmware, and software), their relationship, and their ownership.
- Changes to information systems must follow the ITS Change Management Policy.
- A list mandating approved information technology products will be maintained by the TRU Information Technology Services Division.
- Operational procedures will be made available to all applicable users.
- Capacity management to ensure appropriate usage of resources will be implemented.
- Any testing environments will be managed separately from the main operational network and facilities.
- Any system which stores, processes or transmits Payment Card Industry (PCI) Card Holder Data (CHD) must be located in the TRU data center or be placed in an isolated VLAN designated for the PCI Card Data Environment (CDE).

Vulnerability Scanning & Management

TRU Operations Security Standard

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

- TRU will use a reputable outside source for vulnerability information to be monitored and, as required, a risk ranking will be assigned to vulnerabilities.
- Quarterly internal and external vulnerability scans will be completed by the TRU Information Security Office and an Authorized Scanning Vendor respectively, for the Payment Card Industry Card Data Environments. (PCI CDEs)
- All critical security vulnerabilities in the PCI CDEs will be patched within one month.
- TRU will perform quarterly rogue wireless scans or manual inspections for rogue devices within the PCI CDE.
- Thompson Rivers University will implement controls and processes to properly scan and address vulnerabilities in all information systems at least annually, and when new vulnerabilities appear.
- Appropriate measures should be taken to address associated risks.

Access to Systems

- Two-factor authentication must be used for remote access to the PCI CDEs.
- All visitors to the TRU Data Centre or any other PCI CDE must be authorized by an ITS Manager, wear badges so they are easily distinguished from staff and must sign in and out indicating the firm they represent, and who authorized their access. This entry log will be maintained for a minimum of three months.
- Video cameras or other access control mechanisms must be in place to monitor individual access to areas that house systems which store cardholder data or which store networking gear for the cardholder data environment. This data must be maintained for at least three months.
- Video cameras and electronic access control system must be protected from tampering and disabling.

Managing Point of Sale Devices

- TRU Finance will maintain an inventory of payment devices that includes make/model of the device, location of the device and a unique identifier such as the serial number.
- Payment devices will be routinely inspected for tampering and substitution.

Third Party Service Providers

- TRU maintains a list of all service providers in-scope of PCI.
- The engagement of all service providers must undergo due diligence processes as defined by the TRU Purchasing Department.
- TRU will maintain written agreements with service providers noting they are responsible for the security of PCI CHD whenever it is shared with them.
- TRU will validate the compliance of service providers at least annually.
- TRU will maintain a list of what PCI controls are the responsibility of the service provider and which are the responsibility of TRU.

Protection from Malware

- Protection against malware will be based on malware detection and repair software, information security awareness, and appropriate system access and change management controls.
- Anti-virus software should be deployed on all systems commonly affected by malicious software (particularly, personal computers and servers) and will be monitored to ensure it is current, actively running and generating logs.

- Firewalls must be installed and active on all portable computing devices including employee owned devices.
- Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security standard and unauthorized mobile code shall be prevented from executing.

Backup

- A backup standard must be agreed upon to collect backup copies of necessary data, software, etc. and test them in a timely manner.

Logging and Monitoring

- Information systems should be configured to record all critical systems activities such as login/logout and administrative changes into a log file.
- Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed.
- In addition, the information systems should be configured to notify administrative staff via a Security Information Event Management (SIEM) solution in the event that inappropriate, unusual, and/or suspicious activity is noted.
- All logged access to Card Holder Data (CHD) and logs from devices within the PCI CDE will be reviewed at least daily.
- These logging processes and facilities will be protected accordingly.
- All clocks of the logging and information processing systems will be appropriately synchronized.

Log Retention

- Logs with CHD or Personal Information must be retained for one year.
- The most recent three months of logs must be immediately available for review.

Control of Operational Software

- Thompson Rivers University will maintain controls for the implementation of software and to prevent or detect the use of unauthorized software (e.g. application whitelisting)

Mobile Devices and Teleworking

- Security measures will be developed and adhered to in order to manage risks introduced by the use of mobile devices.
- Security measures will be implemented to protected information accessed, processed, or stored at teleworking/remote sites.

Information Systems Audit Considerations

- Security audits will be conducted annually to ensure information system security controls have been implemented correctly, are operating effectively, and are producing the desired level of security.