RIT | Rochester Institute of Technology

PCI DSS: Third Party Service Provider Policy

1.0 Purpose

- The purpose of this policy is to define requirements for engaging with, monitoring the PCI compliance of, and inventorying all third party service providers that store, process, or transmit payment card data or could impact the security of payment card transactions (TPSP).

2.0 Scope

- This policy applies to all RIT staff and any system that is or will be connected to payment card (credit and/or debit) payment processes.
- This policy applies when adding the ability to accept payments by payment card to a third-party service currently deployed at RIT.

3.0 Policy

3.1. Engagement Procedure

- All RIT staff must follow the Third Party Service Provider (TPSP) Engagement Procedure to get approval from the RIT PCI Team before engaging with a TPSP.
- An IT Risk Assessment must be performed on all services provided by TPSPs or an appropriate exception request must be made to the Information Security Office.
- RIT must develop a written agreement with TPSPs that defines PCI roles and responsibilities. A responsibility matrix can be used to define the details of the written agreement.

3.2 Monitoring

- The PCI Compliance status of all TPSPs must be monitored annually by the PCI Team. The PCI compliance requirements for TPSPs vary based on the service being provided. The PCI Team will determine what is required from TPSPs to validate PCI compliance.
- The PCI Team will review agreements with TPSPs annually. When updates are required, the PCI Team will work to update the written agreement with the Business Unit using the service and the RIT Procurement Services Office (PSO). PSO may require input from the Office of Legal Affairs when updates to written agreements are made.
- If a TPSP fails to validate PCI compliance at any time, the PCI Team may require termination of the service.

3.3 Inventory

- All TPSPs must be inventoried.
- The PCI Team will maintain an inventory of TPSPs, will review the inventory annually, and will update the inventory when changes are made.

3.4 Payment for Services

- Payment for any service provided by a TPSP must be made through a purchase order with PSO, regardless of per monthly/total annual cost.
- Use of RIT procurement credit cards to purchase service from a TPSP is not permitted. All services provided by a TPSP must be paid for on a purchase order issued by the PSO.

4.0 Enforcement

- TPSPs will be reviewed annually for PCI compliance by the PCI Team.
- RIT business units cannot engage with nor continue engagements with TPSPs who are not PCI compliant. If a TPSP is found to be not compliant with PCI requirements, use of the service may be terminated as determined by the PCI Team.
- The RIT Controller's office will not authorize payment for services provided by a TPSP who has not been approved by the PCI Team (at time of initial engagement or after annual review).

5.0 Definitions

- PCI – Payment Card Industry; PCI sets standards that must be followed by all business units who collect payments via payment cards (e.g. credit cards and debit cards)
- Third Party Service Provider (TPSP) – Any third party vendor who provides services that are connected to a payment card process, e.g. Nelnet for online payments, FreedomPay for card-present transactions)
- IT Risk Assessment (ITRA) – RIT's ISO department conducts risk assessments of services being considered. ITRAs are required within the Third Party Service Provider Engagement Procedure and per RIT's Solutions Lifecycle Management Standard
- PSO – RIT Procurement Services Office
- ISO - Information Security Office

6.0 Revision History

- September 2018 – format with new policy template
- November 2024 - deleted associated files section, defined ISO, changed which department performs assessment, and added ISO as part of PCI team.