

# PCI Compliance Quick Start Guide



Information Security Office

City of Austin 2020

# Getting Started

The ISO has been assigned the role of assisting **City Department** with PCI compliance, helping them understand the shared responsibility of PCI compliance and establishing PCI-related processes. As a result, this guide has been made available by the ISO to provide basic knowledge and understanding of payment card industry (PCI) compliance. Use it to get familiar with PCI compliance standards, and as a tool when submitting a completed SAQ to the Information Security Office (ISO).

Before we begin, let's learn a few terms and acronyms:

- PCI: Payment Card Industry – The segment of the financial industry that governs the use of all electronic forms of payment.
- SAQ: Self-assessment Questionnaire – A questionnaire form used as a validation tool intended to assist merchants who self-evaluate their compliance with the Payment Card Industry Data Security Standards (PCI DSS).
- QSA: Qualified Security Assessor – An individual who is PCI-certified to handle compliance auditing and consulting in the payment card industry.
- CDE: Cardholder Data Environment – A computer system or networked group of IT systems that processes, stores, and/or transmits cardholder data or sensitive payment authentication data.

Refer to the PCI SSC site for a complete list of [PCI glossary of terms](#).

## Why Become PCI Compliant

PCI compliance standards have been instituted for the safe transmission of cardholder data during purchases. Without these standards in place, **City Departments** could face penal actions, up to and including indefinite suspension of payment processing capabilities and/or fines.

## When & How to Become PCI Compliant

The **City of Austin** takes PCI compliance seriously. As a result, all **City Departments** are required to become PCI compliant before taking payment for products and/or services.

Before setting up a payment card processing solution, request your merchant ID from the Treasury Department and start gathering the following information:

- Department's CDE description
- Expected number of annual (payment card) transactions
- Device(s) application(s) and connection(s)
- Different ways payments are accepted (e.g., in person, web, IVR, manual)
- Network diagram illustrating payment card security process
- Vendor's PCI compliance-related documentation

Contact the ISO if more information is needed about the above documents and why they're required.

## What's Next

**City Department** should work with ISO to review the selected PCI solutions architecture and determine the correct SAQ for completion.

To learn more about PCI compliance, including merchant level categories, different types of SAQs, and specific compliance standards, visit the following links:

- [PCI Security Standards](#)
- [PCI Glossary of Terms](#)
- [City of Austin Merchant Card Processing Best Practices and Guidelines](#)

Contact the ISO for more information about establishing **your department's** PCI compliance processes.