

Dynamics 365 CE: Payment Card Industry / PCI Compliance Guide

Revision History

v2019-06-14	Joe Clancy	Draft guidance
-------------	------------	----------------

Contents

Controlling documents.....	2
Your commercial relationship with Microsoft	2
The commercial agreement that controls your use of Dynamics 365 is the Microsoft Online Services Terms, together with any amendments you’ve signed.	2
PCI DSS Attestation of Compliance	2
Scope of PCI certification	2
How a customizer can achieve PCC DSS compliance of their solution	2

Controlling documents

Your commercial relationship with Microsoft

The commercial agreement that controls your use of Dynamics 365 is the Microsoft [Online Services Terms](#), together with any amendments you've signed.

PCI DSS Attestation of Compliance

The Dynamics 365 for Customer Engagement Platform has achieved an Attestation of Compliance available in Microsoft's [Service Trust Portal](#), under Trust Documents | Audit Reports | PCI DSS. This Attestation of Compliance relies on the Azure PCI DSS available in the same location, as Dynamics 365 for CE is implemented on Azure's technology stack. You should refer assessors to these documents when undergoing a PCI DSS compliance project when your solution incorporates Dynamics 365 for CE or Azure resources.

Scope of PCI certification

The certified scope for PCI in Dynamics 365 for CE encompasses the underlying data store that persists customer data, the APIs for accessing and managing that data, and customizable portals offering an interface to customer data for end users.

Dynamics 365 for CE does not offer out-of-the-box functionality for storing, processing, or transmitting Cardholder Data. Stated a different way, the Dynamics 365 for CE Platform does not expose built-in use cases such as a Point of Sale terminal, or the checkout and payment functionality of an online shopping experience.

Dynamics 365 for CE offers a platform allowing customizers to build experiences that involve storing, processing, and transmitting Cardholder Data. The data store, APIs, and infrastructure comprising the Dynamics 365 for CE Platform have achieved PCI DSS compliance, and you can build on this platform when certifying your own scenario. You will need to comply with PCI DSS standards when authoring your customizations, and when implementing controls for managing personnel, access control, and auditing.

How a customizer can achieve PCC DSS compliance of their solution

Customizations of Dynamics 365 for CE can include bringing code, schema, business process logic, and administrative controls into your Dynamics 365 implementation. There are PCI DSS controls on each of these, including categories like change management and access control requirements. Composing a plan to satisfy these controls is a project that should be undertaken with your PCI assessor.

Additionally, Dynamics 365 for CE permits administrators to configure numerous types of integration points, offering the ability to connect your D365CE implementation to external systems. Defining the scope of systems and personnel that will be able to access Cardholder Data is an important first step in succeeding at gaining an Attestation of Compliance for your customized scenario.