

What is PCI DSS Compliance?

The Payment Card Industry Data Security Standards (PCI DSS) were developed by all major credit card branding companies including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, Visa Inc, and the PCI Security Standards Council, in order to provide security measures for protecting payment cardholder information and the merchants who store that sensitive information. This multifaceted security standard includes requirements for “security management, policies, procedures, network architecture, software design and other critical protective measures”, according to the PCI Security Standards Council. The Council uses a dynamic approach to maintaining these standards as technology changes and consumer information is compromised. The standard is made up of 12 requirements that, if complied with, will mitigate breaches within the University’s information networks and other secure information storage methods. Higher Education is, unfortunately, one of the highest risk environments for security breaches. Statistically, there are a disproportionate number of breaches occurring at educational institutions within the Payment Card industry. Therefore, PCI DSS is a required standard that **all Universities**, as well as **all merchants, service providers, and banks**, must comply with and is supported by state and federal law. Some of these laws include the Fair & Accurate Credit Transaction Act (FACTA) and the Gramm-Leach-Bliley Safeguards Rule. If a breach occurs, fines can be charged up to \$500,000 which does not include other possible monetary loss due to the breach and the consequences of the information being compromised.

Obtaining and maintaining PCI DSS Compliance is a collaborative effort among several departments at Purdue University. These requirements provide many benefits to our University by making us aware of all sensitive consumer data, not just payment cards numbers. Many processes within the University will become more secure by applying these standards in other areas. We will also be able to maintain processes so that all departments feel secure in accepting sensitive data, and processes will remain consistent, despite employee turn-over.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security