Payment Card Industry (PCI) Data Security Standard (DSS)

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. The payment card brands (Visa, MasterCard, Discover, American Express, and JCB) have collaborated to create a single set of industry requirements, called the PCI DSS, for consumer data protection. The PCI Data Security Standard aligns the security standards to create streamlined requirements, compliance criteria, and validation processes.

University of Colorado departments who accept credit and debit cards for payment are responsible for ensuring all card information is received and maintained in a secure manner in accordance with the payment card industry standards. Individual departments will be held accountable if monetary sanctions and/or card acceptance restrictions are imposed as a result of a breach in PCI compliance.

Below is a high-level overview of the PCI DSS, consisting of 6 goals and 12 requirements:

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 or programs.
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 for all personnel.

For more information, consult the PCI website: https://www.pcisecuritystandards.org/

Also available is a YouTube video about the PCI DSS 12 Requirements:

https://www.youtube.com/watch?v=xpfCr4By71U