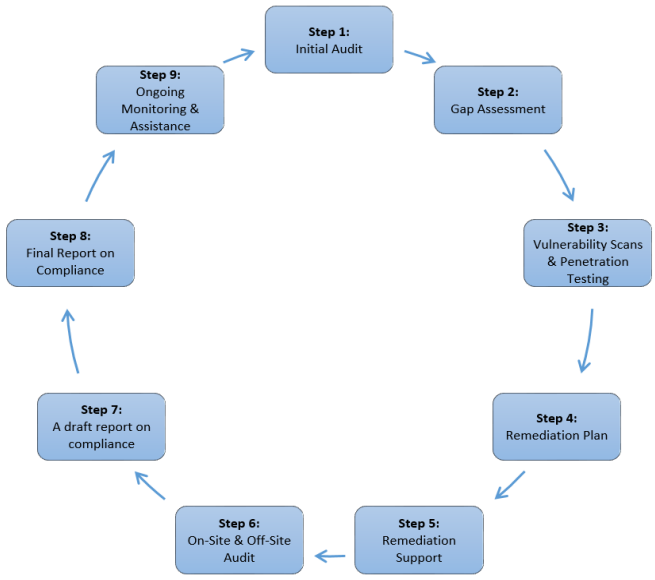
CALIFORNIA STATE UNIVERSITY FULLERTON

Payment Card Industry Data Security Standards

What is PCI DSS?

- Payment Card Industry Data Security Standard (PCI DSS) applies to all entities involved in or affecting the security of storing, processing, or transmitting account data.
- It covers security for any system components included in or connected to a merchant's or service provider's Cardholder Data Environment (CDE).
- The scope of PCI DSS covers the environments receiving account data from payment applications and other sources.
- On-going PCI security maintenance is the key to ensuring the security and integrity of the University Cardholder Data (CHD) and is required to be done annually. On the right is the cycle of PCI compliance.
- For more information on PCI DSS, please visit the CSUF PCI DSS Standards website.



CSUF Involvement

- At Cal State Fullerton, Individual Staff Members, IT Staff, Managers, and Third Party Service Providers (TPSP) are involved in payment card transactions.
- Individual Staff members involved include but are not limited to: Cashiers and Sales Clerks, Call Center Operators, Custodians, Customer Support, Accounting / Finance Personnel, and IT Staff. For more information on Staff members requirements, visit the CSUF PCI DSS Business Standard manual.
- IT Staff include but are not limited to: Data Center Employees, Application & System Developers, Network Operations & Security, and Information Technology & Infrastructure Services. For more information on IT Staff requirements, visit the CSUF PCI DSS Information Security Standard manual.
- Managers include but are not limited to: Department Heads, Information Security Officer, Chief Financial Officer, and Vice Presidents / Presidents.
- Third Party Service Providers include but are not limited to: Transaction Processors, External Sales Agents, Remittance Processing Companies, Payment Gateways, and Offsite Data Storage Facilities.

PCI DSS Six Goals, Twelve Requirements

Goals	*Requirements*
Goal #1: Build And Maintain A Secure Network And Systems	•Install And Maintain A Firewall Configuration To Protect Cardholder Data •Do Not Use Vendor-supplied Defaults For System Passwords And Other Security Parameters
Goal #2: Protect Cardholder Data	•Protect Stored Cardholder Data •Encrypt Transmission Of Cardholder Data Across Open, Public Networks
Goal #3: Maintain A Vulnerability Management Program	•Protect All Systems Against Malware And Regularly Update Anti-virus Software Or Programs •Develop And Maintain Secure Systems And Applications
Goal #4: Implement Strong Access Control Measures	•Restrict Access To Cardholder Data By Business Need-to-know •Identify And Authenticate Access To System Components •Restrict Physical Access To Cardholder Data
Goal #5: Regularly Monitor And Test Networks	•Track And Monitor All Access To Network Resources And Cardholder Data •Regularly Test Security Systems And Processes
Goal #6: Maintain An Information Security Policy	•Maintain A Policy That Addresses Information Security For All Personnel

- For more information on the goals and requirements, visit the PCI DSS Six Goals, Twelve Requirements website.

CALIFORNIA STATE UNIVERSITY FULLERTON

Payment Card Industry Data Security Standards

University Inventory

- The University maintains inventory of all systems and systems that affect the security of storing, processing, and transmitting cardholder data.

Payment Channels

E-Commerce

- E-commerce is the use of the Internet to facilitate transactions for the sale and payment of goods and services.
- For more information, visit the University eCommerce Program website.

P2PE Devices

- P2PE Standard is also designed to support PCI DSS and incorporate PTS, PCI DSS, PA-DSS, and PCI PIN Standards, which may help reduce scope.

For more information on the different types of payment channels and what you may qualify for, please go to the Self-Assessment Questionnaire (SAQ) website.

Skimming

Card skimming is a crime. Using sophisticated skimming techniques, criminals steal or skim data from a customer's card during a transaction using a terminal. More experienced criminals could also attempt to get the customer's PIN at the same time. Once they have this information, it is used in various ways to take money from the customer's account.

Payment card terminals do not save customers' card or PIN details. To skim cards using a terminal, criminals need to apply an overlay, attach external devices such as flash drives, or swap your terminal with one they have already modified. Either way, they need to get access to your terminal.

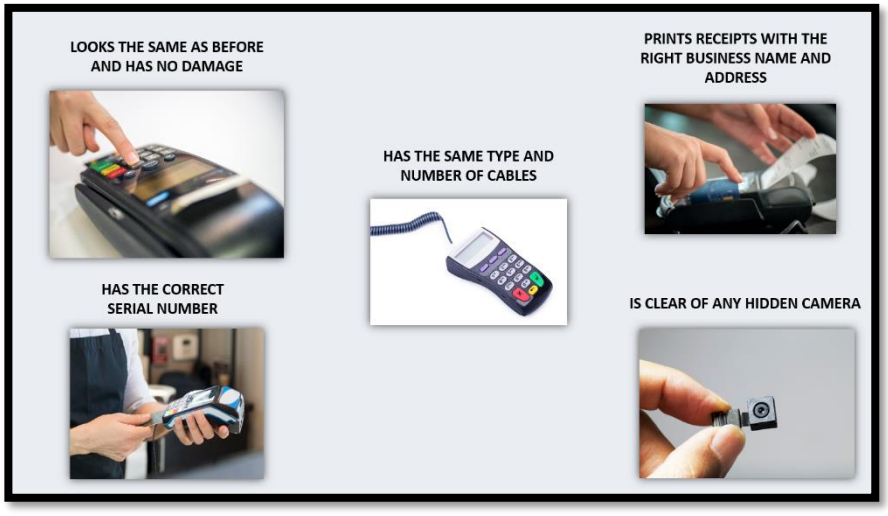
To do this, criminals may:

- Pretend to be a technician that has come to service your terminal.
- Distract you or make a disturbance so that attention is taken away from the terminal.
- Look for a terminal that has been left unattended or is not locked down.

How do I safeguard against skimming?

KNOW YOUR TERMINALS

- Record the following information about your terminals:
  - Brand, model, serial number, and location where a particular terminal is kept in your area.
  - A description of all cables connected to the terminal and details of any security stickers and where they are placed on the terminal.



TAKE ACTION

Be constantly aware of your terminal and how it is being handled - protect it like you would cash. It is preferred that your terminal be physically attached to a counter. If your terminal is not attached to a counter:

- Make sure you put the terminal out of sight and reach of customers if you must leave the immediate area.
- Lock the terminal away at night.

If you see anyone acting strangely near the terminals or security cameras in your area:

- Do not approach the person.
- Watch them closely without putting yourself in danger.
- Contact your supervisor as soon as it is safe to do so.

If you notice anything different or suspicious, take action. **Tell your supervisor immediately.**

BEWARE OF HIDDEN CAMERAS

Be mindful that **criminals may use cameras** to record customers' PINs, so:

- Do not place objects that might hide a pinhole camera near any terminal.
- Ensure that any security cameras adequately cover the terminal area – but are not able to record the PIN entered by a customer.

ACT ON ANYTHING SUSPICIOUS

If any of your staff notice changes to a terminal or suspect a camera may have been used to record PINs:

- Double check all information.
- Disconnect and remove the terminal.
- Store the terminal in a secure location.
- **Immediately report any concerns to the Information Security Office at iso@fullerton.edu and DL-PCICC@fullerton.edu.**

VERIFY SERVICE VISITS

Staff should direct all visits by technicians and other service contractors to a supervisor. **All visitors should be asked to present their security identification (ID).** If the visit was not booked, or the ID does not match arrangements, contact Supervisor.