PCI is a credit card account number alone or with any of the following:
  • Cardholder name
  • Service code
  • Expiration date

PCI Safeguards:
✓ Do not access PCI without authorization
✓ Access PCI only using authorized applications
✓ Report exposed data immediately to the UF Privacy Office
✓ Never transmit PCI in:
  o Email
  o Instant messages
✓ Never store PCI on:
  o A desktop computer
  o Any computer that is not professionally managed, such as your home computer
  o A Laptop, PDA or smart phone or other portable devices
  o Removable media such as CDs, DVDs and USB thumb drives
✓ Regardless of the use, practice the following safeguards
  o Obtain approval for all devices, media and software used with PCI
  o Use strong passwords to access PCI
  o Password-protected screensaver with a short time-out
  o Minimize the amount of data stored
  o Minimize the length of time data is stored
  o Encrypt stored data, preferably using whole-disk encryption
  o Only use applications that encrypt transmitted data
  o Encrypt backups and minimize backup retention time
  o Render all media unreadable prior to reuse or disposal