What is PCI?

- Payment Card Industry (PCI) Standard
- Required compliance for all merchants that process, store or transmit credit card information maintain a secure environment.

The standard can be found on the PCI Security Standards Council’s Website:
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
Why Do We Need To Be Compliant

- Protect citizens and employees from fraud, identity theft
- Protect the City's assets
- Protect the City's reputation
IT Responsibilities

1. Managing the network and access for City PCI devices to support PCI compliance
2. Assisting and approving departments in equipment/software and technical design
3. Assist departments PCI compliance issues
Department Responsibilities

1. Ensure all staff are properly trained and aware of PCI procedures
2. Develop PCI procedures for the department and/or location
3. Enforce IT Security policies
4. Enforce PCI procedures
5. Ensure that physical locations are secure
6. Track all inventory and staff resources involved in the payment card process
7. Ensure all PCI devices are scanned and adhering to requirements
8. Maintain all department documentation for any PCI audits and produce documents
Who Needs PCI Training?

• Any city employee, contractor or other individual that takes or processes credit cards from the general public or other employees

If you operate a cash register and/or take any credit card payments you need to take training
What Do I Need To Protect?

1. Cardholder Data
2. Equipment & Facilities
   - Card Readers
   - Cash Registers
   - Facilities Using Credit Cards
   - Equipment/Networks Transmitting CC Info
3. Software and Log Ons
Cardholder Data
Cardholder data includes the primary account number (PAN) along with any of the following data types: cardholder name, expiration date or service code. A service code is a three- or four-digit number on cards that use a magnetic-stripe. The service code specifies acceptance requirements and limitations for a magnetic-stripe-read transaction.

If the cardholder name, expiration date and/or service code are stored, processed or transmitted with the PAN, they must be protected in accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements.
Many banks insist that their merchants retain complete records of all credit card transactions in case there is a disputed transaction. However, all the merchant needs is the authorization number from the processor, the dollar amount and to have checked the customer's identification for a card present transaction, or to get the card verification value code and billing zip code for a card not present at the transaction.
What Data Do I Not Keep?

- Avoid writing down, copying, storing, or otherwise keeping any cardholder data for any record, transaction or correspondence.
- Do not send credit card information through any electronic process. E-mail, text, attachments
- Do not implement any system, process or service that requires the storage of cardholder data on a City PC, server, mobile device or paper.
Equipment & Facilities
Inventory of Devices

• Keep an up to date inventory of all devices capable of taking credit card payments.
  – Device Type
  – Location (Address, Floor, Room, Desk)
  – Serial number or unique identifier
  – Make
  – Model
Update the Inventory

- Do a physical inventory annually of devices
- Update the inventory list when devices are added, relocated or decommissioned.
  - Document when this takes place
- Have up to date manuals/documentation of all readers and devices in a secure locations
Inspect Devices

- Inspect the devices each day
  - Correct serial number (ensure no swap out)
  - Wiring has not been tampered or moved
    - Wires sticking out of the reader
  - Is the reader loose or damaged
  - Any tape or residue on the slot
  - Skimmers or other devices have been attached
  - Anything that looks out of the ordinary
    - Missing or changed labels
    - Different color or shape
Actual card reader

Modified Card Reader

Skimming unit snaps in place over existing card reader, reading card while allowing ATM to function
Look for loose wires and tape
BE CAREFULL !!
SPOTTED IN SHANGHAI - ATM SKIMMER TO COPY AND DEFRAUD YOU

Unfitting gap
Superglue !!
Overlapping arrow
glue trace
Secure Facilities

- Lock up the area or readers when not in use
- Never leave readers unattended where the public may have access
- Server/Network/Telco Rooms
  - Locked at all times
PC/Server Requirements

- Vulnerability Scans Monthly
- Anti Virus Software Installed & Maintained
- Only Payment Application On PC (no e-mail, Internet Surfing, etc.)
- Critical Security Patches Up To Date, Installed within 1 Month of Release
- Supported Operating System, Software and Hardware
- Intrusion detection for each PC/Server
- IT may approve and inspect any PCs and Servers
Do not attach devices to the network without IT notification and coordination.

Do not utilize mobile payment card devices without IT notification and coordination.

IT will install and configure all network devices.

Do not install unauthorized wireless access points and devices in the facility.
  - Report any unauthorized wireless access points immediately.

Do not plug thumb drives, storage devices, printers or other devices to a payment device without authorization.
Users Requirements
Respond to Suspicious Activities

• Verify the identity of any 3\textsuperscript{rd} party repair & maintenance personnel \textbf{before} granting access
  – Make sure your supervisor is aware and there was a known service call
• Report and suspicious behavior around devices (attempts by unknown persons to unplug or open devices)
• Report suspicious behavior and indications of device tampering or substitution to your PCI coordinator
Only employees that perform transactions should have a log on or access payment processing devices

- Access assigned based on employee function & classification

Passwords changed every 90 days

Do not share your password information with anyone

Do not leave payment devices unattended in a public area

Log off the system when you leave the device

Do not install, replace or return devices without verification from your supervisor/manager