UCT Support Procedures for Ensuring PCI-DSS Compliance

Introduction

The University of Houston Clear Lake requires any system that takes a credit or debit card for payment to comply with the Payment Card Industry's Data Security Standard (PCI-DSS). To ensure that this requirement is met, any system implementation that involves credit or debit card payments must be reviewed and approved by the University's Information Security Officer. Additionally, any system that involves University computers or networking equipment must be approved by the University's Chief Technology Officer.

When any University staff member submits a request to UCT/Support Services involving the implementation of any manual or automated system that accepts credit/debit card payments, UCT/Support Services will direct that individual to the University's Information Security Officer.

The University's Information Security Officer will work with the requestor, the University's Chief Technology Officer and the appropriate members of the UCT staff, UHCL Finance and UH System to ensure that PCI-DSS compliance issues are addressed, and any solution proposed complies with UHCL and UH System policies, and is compatible with our technology infrastructure, facility constraints, procedures and standard business practices.

NOTE – IF THE REQUEST IS APPROVED, BEFORE PROCEEDING, THE REQUESTING DEPARTMENT MUST AGREE TO BE RESPONSIBLE FOR THE FOLLOWING ON AN ONGOING BASIS:

- ***PROVIDING FUNDING FOR ALL THE EQUIPMENT AND SERVICES REQUIRED TO ACHIEVE PCI-DSS COMPLIANCE.***
- ***ENSURING THAT EVERY EXTERNAL ORGANIZATION THAT COMES IN CONTACT WITH THE DEPARTMENT'S CUSTOMERS' CREDIT/DEBIT CARD INFORMATION IS CERTIFIED AS BEING PCI-DSS COMPLIANT ON AN ANNUAL BASIS.***
- ***COMPLETING THE APPROPRIATE PCI-DSS SELF-ASSESSMENT QUESTIONNAIRE AND ATTESTATION OF COMPLIANCE ON AN ANNUAL BASIS OR WHEN OTHERWISE REQUIRED.***

There are a variety of ways that systems can accept credit or debit cards for payment that are described in the next section of this document.

Examples of Credit/Debit Card Payment Solutions

Below is a description of common credit card processing scenarios and the steps that UCT will take to ensure that the system and business procedures keep the University in compliance with PCI-DSS. Please note that the list is not exhaustive.

SCENARIO 1 – THE USE OF A CREDIT CARD TERMINAL DEVICE THAT IS APPROVED BY THE UH SYSTEM TREASURER'S OFFICE AND COMMUNICATES VIA DIAL-UP OR CELLULAR CONNECTION (PREFERRED)

DESCRIPTION

- The agreed upon solution uses a PCI-DSS compliant third party vendor to process credit card data.
- The credit card data is entered into a University-based credit/debit card terminal device that is capable of communicating directly with the University's payment processor and is approved by the University of Houston System's Treasurer's Office.
- The terminal device communicates directly with the payment processor via either via a physical dial-up line or a cellular signal.

WHAT UNIVERSITY EQUIPMENT IS "IN-SCOPE" FOR PCI-DSS COMPLIANCE?

- Only the terminal devices.

THE REQUESTING DEPARTMENT IS RESPONSIBLE FOR:

- Purchasing one or more terminal devices that are approved by the UH System Treasurer's Office.
- Paying any maintenance charges associated with the terminal device
- Paying the cellular account charges that cover the use of transmit the credit/debit card data to the payment processor.
- Confirming that the third party vendor remains PCI-DSS compliant annually.
- Ensuring that PCI-DSS procedures and business practices are followed by departmental staff.

UCT IS RESPONSIBLE FOR:

- Assisting with the installation of a dial-up line, if applicable.

SCENARIO 2 – THE USE OF AN IN-HOUSE DEVELOPED OR PURCHASED APPLICATION THAT DOES NOT COLLECT CREDIT/DEBIT CARD DATA ON ANY UNIVERSITY COMPUTER (PREFERRED)

DESCRIPTION

- The solution uses an off-site PCI-DSS compliant third party vendor at least for the portion of the application that collects and processes credit card data that is entered by the customer into a device of his or her own choosing.
- Other portions of the system, e.g., those that allow the customer to select products or services for purchase, may be performed by application software residing on University computers or may be hosted off-site.
- No member of the University staff or faculty associated with the system may enter credit/debit card data on the customer's behalf or direct the customer to use a specific University computer.

WHAT UNIVERSITY EQUIPMENT IS "IN-SCOPE" FOR PCI-DSS COMPLIANCE?

- No University equipment is in scope.

THE REQUESTING DEPARTMENT IS RESPONSIBLE FOR:

- Obtaining a merchant account from Finance or the Treasurer's Office.
- Working with UCT's Application Development team to develop the in-house, non-credit/debit card processing functions and those that reroute the customer to the payment processor's site.
- Confirming that the third party vendor remains PCI-DSS compliant annually.
- Ensuring that PCI-DSS procedures and business practices are followed by departmental staff.

UCT IS RESPONSIBLE FOR:

- Providing development, networking and server support resources as necessary.
- Supporting the portions of the application software that reside in-house, and the servers and networking equipment involved.
- Working with the requesting department and the external organization that processes the credit/debit card payments to resolve interface issues.

SCENARIO 3 – THE USE OF IN-HOUSE DEVELOPED OR PURCHASED SOFTWARE THAT DOES NOT STORE DATA ON UNIVERSITY SERVERS, BUT DOES USE SPECIFIC UNIVERSITY COMPUTER(S) TO COLLECT CREDIT/DEBIT CARD DATA (GENERALLY DISCOURAGED DUE TO HIGHER RISK THAN SCENARIOS 1 AND 2)

DESCRIPTION

- The solution uses a PCI-DSS compliant third party vendor to collect and process credit card data.
- While credit/debit card transactions may be entered by customers a majority of the time, there are occasions when transactions may be:
    - Entered into a University computer by an authorized member of the University's staff or faculty, or
    - Entered by the customer into a University computer to which he or she was directed by department staff or faculty.

WHAT UNIVERSITY EQUIPMENT IS "IN-SCOPE" FOR PCI-DSS COMPLIANCE?

- The computers used to enter the transactions
- Any network to which each computer is connected and any network beyond that until a firewall that can control access to the computer is reached
- Any computer on the aforementioned "in-scope" networks.

THE REQUESTING DEPARTMENT IS RESPONSIBLE FOR:

- Obtaining a merchant account from Finance or the Treasurer's Office.
- Purchasing a firewall/router.
- Covering networking costs associated with configuring and operating their PCI system.
- Providing secure space for any University-based hardware that is involved in the credit/debit card payment process. The space must be secured against access by unauthorized individuals.
- Physically securing any University workstation that collects credit/debit card data when not in use, and designating the devices "for PCI use only."
- Confirming that the third party vendor remains PCI-DSS compliant annually.
- Ensuring that PCI-DSS procedures and business practices are followed by departmental staff.

UCT IS RESPONSIBLE FOR:

- Hardening the workstations that will be used to enter credit/debit card data to comply with PCI-DSS rules.
- Providing network connectivity between the firewall/router and the University's Internet-only VLAN.
- Providing a single routable IP address for all devices on the protected VLAN that the firewall/router will NAT (Network Address Translation) to the individual non-routable IP addresses assigned to each workstation that will be used for credit/debit card data entry.
- Configuring the firewall/router and ensuring the device is appropriately secured before activating.
- Providing support for the workstations as with normal computing support.
- Creating and maintaining a separate PCI-DSS compliant image with only browser and, if needed, printing capabilities.
- Maintaining security patches and updates within 2 weeks, with exception for cause.
- Creating local accounts for each user of the machine or a generic account for kiosk type machine.
- Supporting only the portions of the applications reside on University servers, the server operational software, and the server hardware. UCT will not support portions of the application that are hosted off-site. Such support requests should be directed to manufacturer and/or vendor.
- Participating in the development and vetting of PCI-DSS compliant system designs, business procedures and best practices.

SCENARIO 4 - THE USE OF PURCHASED SOFTWARE THAT STORES DATA ON UNIVERSITY SERVERS, EVEN TEMPORARILY (HIGHLY DISCOURAGED DUE TO ITS SIGNIFICANT RISK AND COST OF COMPLIANCE.)

NOTE – EVERY EFFORT MUST BE MADE TO HAVE THE VENDOR TRANSFER THE APPLICATION'S CREDIT/DEBIT CARD COLLECTION AND STORAGE RESPONSIBILITIES TO THE UNIVERSITY'S PREFERRED PAYMENT PROCESSOR.

DESCRIPTION

- The system is purchased from a PCI-DSS compliant vendor.

NOTE – DEVELOPING ANY SOFTWARE "IN-HOUSE" THAT STORES DATA ON A UNIVERSITY SERVER IS NOT ACCEPTABLE.

- The credit/debit card payment system resides on University servers, including the portions of the application that collects the credit/debit card information either from the customer or from departmental staff or faculty on the customer's behalf.
- Credit/debit card information is stored, even temporarily, on University servers, either on disk or in memory.

WHAT UNIVERSITY EQUIPMENT IS "IN-SCOPE" FOR PCI-DSS COMPLIANCE?

- Every piece of University networking equipment that is not firewalled away from the network housing any device that touches credit/debit card information.
- Every University computer that is not firewalled away from the network housing any device that touches credit/debit card information.
- Every University server and workstation that touches credit/debit card information.
- In addition to the aforementioned equipment, the following is also in scope:
    - The University's data center and communications closets,
    - Our operational practices,
    - Our change management practices,
    - Our personnel hiring practices, and more.

THE REQUESTING DEPARTMENT IS RESPONSIBLE FOR:

- Obtaining the approval of the University's Information Security Officer, the University's Chief Technology Officer, the Chief Information Security Officer of the University of Houston System, and UH System's General Counsel.
- After all approvals are obtained,
    - Obtaining a merchant account number from Finance or the Treasurer's Office.
    - Working with UCT to plan the implementation, install the software and test the purchased software.
    - Establishing PCI-DSS compliant procedures and business practices.
    - Ensuring that PCI-DSS procedures and business practices are followed by departmental staff.

UCT IS RESPONSIBLE FOR:

- Providing implementation planning, administrative, operational and maintenance support for the application.

SCENARIO 5 – ALLOWING A UNIVERSITY BUSINESS PARTNER TO IMPLEMENT A SYSTEM ON-CAMPUS THAT ACCEPTS CREDIT/DEBIT CARD TRANSACTIONS FOR PAYMENT AGAINST THEIR OWN MERCHANT ACCOUNT (GENERALLY DISCOURAGED DUE TO POSSIBLE RISKS)

DESCRIPTION

- An on-site University service provider (USP), such as, Aramark, needs to deploy a system that resides on University property, and uses the University's networking equipment.
- The USP bears all system-related costs.
- Connectivity to the Internet is provided in one of two ways:
    - The best solution would be for the USP to purchase its own Internet connection (e.g., DSL line) into the University that would be used exclusively to connect their point-of-sale devices to the system provider and/or payment processor, off-campus. This would remove all University computers and network equipment from being in scope for PCI-DSS compliance.

- If the external Internet connection cannot be obtained in a timely manner, the University may provide Internet connectivity temporarily by serving as the ISP for the implementation.

NOTE – A PLAN FOR MOVING THE INTERNET CONNECTION FROM THE UNIVERSITY'S NETWORK TO A SEPARATE USP CIRCUIT IN A REASONABLE TIMEFRAME MUST BE PROVIDED BEFORE ANY APPROVALS ARE GRANTED.

WHAT UNIVERSITY EQUIPMENT IS "IN-SCOPE" FOR PCI-DSS COMPLIANCE?

- No University equipment is in scope as long as the University at most acts solely as the USP's Internet Service Provider (ISP), and no device behind the University service provider's firewall is also used for University purposes.

THE USP IS RESPONSIBLE FOR:

- Obtaining the credit/debit card merchant account.
- Purchasing, administering, operating and maintaining the system.
- Working with UCT networking personnel to completely isolate the system from the University's servers and workstations and the University's networks through the use of a firewall/router owned, administered and maintained by USP personnel. This implies that no communications are permitted between any USP device and any University device, except for the networking equipment that takes USP data from its firewall/router to the Internet, and vice versa.
- Placing its own firewall/router at the de-marc point between our network connection and theirs.
- Assigning and maintaining the non-routable IP addresses for the equipment on their network and of the NAT process that associates the routable and non-routable IP addresses.
- Maintaining PCI-DSS compliance for its systems, procedures and business practices, and does not hold the University accountable for any PCI-DSS responsibilities.

UCT IS RESPONSIBLE FOR:

- Providing connectivity between the USP's devices and the Internet, if necessary.
- **IF THE UNIVERSITY PROVIDES INTERNET CONNECTIVITY,**
  - Ensuring that the least number of University devices possible are used to provide Internet connectivity.
  - Providing the minimum number of routable IP addresses necessary for the USP's credit/debit card operation.

- Ensuring firewall/router rules prevent the USP's devices from directly accessing anything on the University's network other than services available to the general public.

- Adding access restrictions to the University's firewalls/routers to provide additional protection for the USP's system.

NOTE – THE ABOVE ACCESS RESTRICTIONS MAY NOT BE USED TO SATISFY ANY PCI-DSS REQUIREMENT THAT HAS NOT BEEN SATISFIED BY THE USP.

- Responding to USP support requests that are associated with the quality of the network connection to the Internet. UCT will not provide any support for the USP's hardware or software.