Requirements & Potential Costs for SAQ D

The University of Utah prefers to use vendors who provide web host based (Cloud) payment card processing or who will redirect the payment portion of the software to a hosted order page or other hosted payment card processing method. These processing methods keep all credit card data from passing through University servers.

If your vendor software captures payment card data to pass on to a gateway, the data will be passing through a University server and will be in scope for the entire Payment Card Industry Data Security Standard. The requirements for this standard may cost your department additional, one time and annual fees. These fees include, and are not limited to:

- Application and System logging $ per year
- PCI Segment for all applicable devices
  - Workstations
  - Servers
- Penetration Testing
- Annual Compliance Assessment
- Data Center Security

Checklist for Implementing Third Party Processing:

*The following items must be completed **before going live** with your Third Party Vendor Implementation. If you have any questions regarding these items please contact us. Use this checklist to track the progress of your application.*

Complete the following before submitting request:

☐ Contact Purchasing to see if a RFP is required.

☐ Obtain Data Flow Chart from Third Party Vendor.

☐ Obtain the Vendor's signed Attestation of Compliance (AOC).

☐ Complete the following "Request for Using a Third Party Vendor Form".

☐ Complete the "Information Sharing Assessment" form for remote access by the Vendor (if applicable).

Before Going Live:

☐ Submit Third Party Contract or Addendum to Legal Counsel for review. Complete *Attestation #3 – Confirmation of Legal Counsel Review*. Give copy of contract and Attestation #3 to Income Accounting and Student Loan Services.

☐ Complete Internal Scan; fix any associated issues (if applicable).

☐ Complete applicable testing, including end to end encryption testing, or penetration testing.

☐ Complete the Department Payment Card Acceptance Procedure and Employee List.

☐ Complete PCI DSS Annual Training – include all staff involved in maintaining the Third Party System, and those who will run transaction, and those who supervise those who run transactions.

Notes:

Contacts:

Security Scans/ Technical Advice
Michael Adair
587-6198
Michael.Adair@hsc.utah.edu

PCI DSS Compliance
Kim Stringham
585-5686
Kim.Stringham@utah.edu

Income Accounting, Assoc Director
Lisa Zaelit
581-3968
Lisa.Zaelit@admin.utah.edu

Merchant Account – Request for Approval for a Third Party E-commerce Vendor

Attn: Kim Stringham Fax to 801-585-3898

Date: _____

Department Name: _____

Address: _____ City: _____ St: _____ Zip: _____

Contact Name: _____ Phone #: _____ E-Mail: _____

ORG Head: _____ Phone #: _____ E-Mail: _____

Dean/VP/ Chair: _____ Phone#: _____ E-Mail: _____

Data Steward: _____ Phone #: _____ E-Mail: _____

Data Custodian: _____ Phone #: _____ E-Mail: _____

System Administrator: _____ Phone #: _____ E-Mail: _____

Provide the following checklist items and complete the questions below:

☐ Provide detailed data flow chart and complete *Addendum 1 – Attestation: Complete Disclosure Flow Chart.*

☐ Copy of Third Party Contract – existing or pending.

☐ Copy of PCI Certificate and/or appropriate certification (can include a copy of their recent SAQ or Attestation of Compliance & Recent Scan Report, or recent Executive Summary).

☐ Complete *Addendum 2 – Attestation: Prohibitive Data Retention* (if applicable).

☐ If you will be accepting donations, provide a list of the information you will be collecting and/or storing.

☐ Name and phone number of the ***Technical Contact*** for the Third Party Vendor(s). _____

_____

- **Please describe the business need for accepting credit cards and why the selected vendor best meets the department's needs:**

- **Why will the approved payment applications (i.e. UMarket, Third Party Vendor list, electronic equipment) not meet your needs?**

- **What is the name of the Third Party Vendor(s) (Company Name, Distributer, or Service Provider)?**

- **What is the name of the Payment Application the Vendor is providing for you?**

- **Is there another name for the product?**

- **Does the payment application use a separate gateway? ☐Yes ☐No**
  If yes, what is the name of the gateway?

- **Will the card information <u>pass through</u> a University Server? ☐Yes ☐No**
  What is the IP Address(es)? _____
  _____
  _____

  Please describe the flow of information:

- **Is card information or other sensitive data <u>stored</u> on a University Server or the Third Party Server? ☐University Server ☐Third Party Server. Please provide a flowchart that shows information pass through and storage.**

IPs & Flow Chart Reviewed by: _____ _____ Dan Bowden, CISO 213-3397 Date

- **Does the vendor have a Re-Direct option (software takes the customer to a hosted order page to gather credit card data)? ☐ Yes ☐ No**

  If yes, will you be using this option? ☐ Yes ☐ No

- **Describe your implementation timeline and indicate any business-critical dates:**

- **Does the new system replace any existing systems or processes?**

- **Do you anticipate either extracting data from PeopleSoft or passing data to PeopleSoft? If so, please describe how you envision that working:**

- **Can the vendor use a Wells Fargo (FDMS) merchant account? ☐ Yes ☐ No**

- **Is the Third Party Vendor(s) and/or Payment application(s) PCI DSS Compliant?**
  Please attach PCI DSS Attestation of Compliance (AOC)
  ☐ Yes ☐ No If No, please explain what measures they are taking to become compliant:

- **Is this an existing program or system in your department? ☐ Yes ☐ No**
  If yes, is payment card acceptance an additional feature that requires a contract addendum? ☐ Yes ☐ No
  If yes, who signed the contract and/or addendum: Date:

- **If this is a new contract, has it been reviewed by General Counsel? ☐ Yes ☐ No**
  ☐ In Process Which VP or VP designee will sign the contract?

- **Will you be accepting donations? ☐ Yes ☐ No If yes, will the donor information be stored on a University system? Please describe.**

Please submit this completed form with the items requested in the checklist above, to Income Accounting and Student Loan Services, Rm. 155 Student Services Building, Attention: Kim Stringham.

Contact Name: _____ Signature: _____
Print

ORG Head Name: _____ Signature: _____
Print

Third Party Authorization:

☐ Approved ☐ Declined

_____ _____

Laura Howat, Controller for University of Utah, Financial Business Services Date

Explanation and/or Conditions: _____

Attestation 1: Complete Disclosure Flow Chart

This document must be completed by the Department to demonstrate the proposed Third Party Vendors compliance with the Payment Card Industry Data Security Standard (PCI DSS), and the Department's compliance with the University of Utah's Payment Card/E-Commerce Policy. Submit to Income Accounting and Student Loan Services.

_____ _____

Merchant/Department Name *Date*

Merchant Confirms:

☒ The submitted data flow chart fully and correctly discloses all vendors and methods involved in processing cardholder information.

☒ The submitted data flow chart accurately and completely discloses the flow of data from front end user to the capture and settlement of the transaction.

Contact Name: _____ Contact Signature: _____
(Print)

Date: _____

Org Head Name: _____ Contact Signature: _____
(Print)

Date: _____

Attestation 2: Prohibitive Data Retention

This document must be completed by the Department to demonstrate the proposed Third Party Vendors compliance with the Payment Card Industry Data Security Standard (PCI DSS), and the Department's compliance with the University of Utah's Payment Card/E-Commerce Policy. Submit to Income Accounting and Student Loan Services.

_____ _____

Merchant/Department Name *Date*

Merchant Confirms:

☒ No evidence of magnetic stripe (i.e., track) data, CVV2 data, or PIN data will be stored on a University of Utah server/computer.

☒ No cardholder data, including card number and expiration date, will be stored on a University of Utah server/ computer.

Contact Name: _____ Contact Signature: _____
(Print)

Date: _____

Org Head Name: _____ Contact Signature: _____
(Print)

Date: _____

Attestation 3: Confirmation of Legal Counsel Review

This document must be completed by the Department to demonstrate that University Legal Counsel has reviewed the Third Party Vendor Contract prior to signing. An email from the reviewer should be attached. All Third Party Vendor Contracts must be signed by a Vice President for the department, or by the Vice President's Designee.

_____ _____

Merchant/Department Name *Date*

Merchant Confirms:

☐ The Third Party Contract for the applicable merchant services has been reviewed by University Legal Counsel.

☐ An email or other document from University Legal Counsel is attached, which states the Third Party Contract has been reviewed.

☐ A copy of the signed contract will be sent to Income Accounting and Student Loan Services.

Contact Name: _____ Contact Signature: _____
(Print)

Date: _____

Org Head Name: _____ Contact Signature: _____
(Print)

Date: _____

INFORMATION SECURITY AND PRIVACY OFFICE
THE UNIVERSITY OF UTAH

Information Sharing Assessment

A Business Associate Agreement (BAA) is required when information is shared with a company or person who is not a member of the U of U or UUHS workforce AND who, on behalf of the U of U or UUHS performs, or assists in the performance of, an activity involving the use or disclosure of sensitive data or protected health information.

This assessment must be completed prior to entering into a Business Associate arrangement.

Completion of this process may take up to 3 weeks after signed BAA is received from vendor.

We will notify you when the BAA has been fully executed and our website updated.

If you have any questions, please contact us at (801) 587-9241.

1. Will University information/PHI be sent to a third party, or will the third party have access to systems at the University?

2. What is the third party doing for us or on our behalf where this information needs to be shared?

3. How will the information be accessed, sent to, and received from, the third party?

4. Is access to this data or system critical for the performance of your own, or your departments, job functions?

5. Which of the options below best describes the University of Utah's relationship with the third party/vendor:

   _____ The vendor will be working with data on-site at the University of Utah and will never access it remotely or remove it from the premises.
   _____ The vendor will be working remotely with University of Utah data and/or will be transporting or transmitting University of Utah data to and from a remote site.
   _____ The vendor will be hosting software that you will access (i.e., software as a service, web hosting, etc.).
   _____ Other, please describe:

6. Please complete the following information:

Department Name	
Point of Contact	
Phone & Email	
Vendor Name:	
Address:	
City:	
State, Zip Code:	
Point of Contact	
Phone Number:	
Email Address:	