UNIVERSITY OF OREGON Business Affairs Office

Clear Form

UO Third Party Credit Card Processing Request

To protect customer cardholder data and comply with Payment Card Industry (PCI) rules, Third Party Service Providers and Payment Applications used to process credit card payments to the university, must be approved by Business Affairs before contracting or purchase.

1. Third Party Information

Company Name: _____

Address: _____

Website: _____

Contact Name: _____

Contact Title: _____

Contact Phone: _____

Contact E-mail: _____

2. Product or Service

Check the box next to the description that best illustrates your organization's product or service.

☐ Service Provider provides fully hosted payment processing services. Cardholder data is stored, processed and/or transmitted using the Service Provider's network. No cardholder data is stored, processed and/or transmitted on the university network.

☐ Vendor provides, a payment application that will be hosted and maintained by the university. Payment application name and version,

_____

☐ Other, describe

3. Flow of Cardholder Data

Describe flow of cardholder data for a single transaction (attach illustration of all systems involved in processing an order. Indicate which organization owns and maintains each system. Identify any independent 'nested' service providers involved in the transaction.

4. Flow of Funds.

Describe the flow of funds for a single transaction. Indicate the maximum elapsed time from payment to university receipt of funds.

If E-check transactions will be processed they must post to university and customer bank accounts on the effective date of the transaction, e.g.., the transaction must credit the university account on the same day that it debits a customer's account. If applicable; describe how your solution will meet this requirement.

5. Merchant ID

Credit card sales will, (check the box that best describes MID ownership)

☐ Be deposited directly into a UO merchant account (MID). The university is the merchant of record responsible for the security of cardholder data.

☐ Be deposited directly into the vendor's MID. The Vendor is the merchant of record responsible for the security of cardholder data.

Your company is certified and processes directly with:

☐ Elavon and/or
☐ TSYS

OR

Your company uses a PCI-compliant payment application/gateway to process through:

- ☐ Elavon and/or
- ☐ TSYS

List the payment applications/gateways your service uses to process through Elavon and/or TSYS.

Please note: The major card brands and the university's merchant bank require unique merchant IDs for:

a) Each physical address
b) Internet transactions
c) Point of Sale (POS) or card present transactions
d) Mail Order/Telephone Order transactions (MO/TO) if over 20% of all transactions.
e) Each Merchant Category Code (MCC)

6. PCI Compliance

Check the box next to the description that best illustrates your organization's product or service.

☐ Level 1 Service Provider listed on the Visa Global Registry of service providers.

☐ Level 2 Service Provider contracted with a Qualified Security Assessor (QSA) to perform a Report on Compliance (ROC) that validates PCI DSS compliance.

Qualified Data Security Company: _____

Primary Contact Name: _____

Primary Contact Number/e-mail: _____

Date Assessment was Completed: _____

☐ Payment Application included on PCI Standards Council list of validated payment applications. Application installed and configured by a qualified integrator in a PCI compliant fashion.

☐ Other, describe

Per PCI DSS requirement 12.8.5 please attach a list of PCI requirements identifying which party is responsible for each, (the vendor, the university, or shared by both parties).

☐ Check this box to acknowledge that the following text will be executed as an addendum to the vendor contract;

In accordance with PCI DSS 12.8.2 vendor acknowledges,

a) *Responsibility for the security of cardholder data it possesses or otherwise stores, processes or transmits on behalf of the University of Oregon, or to the extent that vendor could impact the security of the cardholder data environment.*
b) *Sole responsibility for all requirements contained in the Payment Card Industry Data Security Standard (PCI DSS) and/or Payment Application Data Security Standard (PA DSS).*

Vendor attests that,

a) *It has complied with all applicable requirements contained in the current version of PCI DSS and/or PA DSS,*
b) *It has performed the necessary steps to validate its compliance, and*
c) *It will remain in compliance for the life of this Addendum.*

Vendor will,

a) *Supply evidence of its most recent validation of compliance upon execution of this addendum and annually for the length of the contract,*
b) *Notify University of Oregon within seven days if it falls out of PCI DSS or PA DSS compliance, and provide a remediation plan and timeline.*
c) *Notify University of Oregon within 24 hours if it detects unauthorized access to customer card data.*
d) *Provide representatives of University of Oregon with full cooperation and access to conduct a security review in the event of unauthorized access to cardholder data.*
e) *Comply with all applicable laws requiring notification of individuals in the event of unauthorized access to cardholder data.*
f) *Indemnify, hold harmless, and defend the University and its employees from and against any claims, damages, or other harm related to a breach. This provision survives termination of the contract.*

Vendor acknowledges that unauthorized access to cardholder data resulting from a lapse in Vendor's security obligations is grounds for early termination of this agreement without penalty, at the University's discretion.

7. Third Party Vendor Fees

The university does not allow any organization to debit its bank accounts by ACH for fees.

☐ Checking this box indicates that you or another organization working on your behalf will invoice the university for fees associated with the services you provide.

List all parties involved in the fee process, fee amounts, and how the fees will be collected:

8. Certification

By signing this document, you certify that your answers are complete and correct to the best of your knowledge, and accurately reflect your organization's actual practices, policies, and procedures.

Signature: _____

Name: _____

Title: _____

Date: _____