**CampusGuard Merchant Survey Template**

1. **Merchant Information:**

|  |  |
| --- | --- |
| Merchant Department: |  |
| Merchant Address (Location): |  |
| Department ID: |  |
| Merchant ID (MID#): | See below |
| Merchant Name or DBA: | See below |
| Merchant Division Name: |  |
| Merchant Website: |  |
| **Online ACH:** |  |
| **Dept. Description:** | Please add content here. |

**Note: Additional MID information should be populated on page 6.**

1. **Primary Contact/Merchant Manager Contact Information:**

|  |  |
| --- | --- |
| Primary Contact Name: |  |
| Contact Title: |  |
| Phone Number: |  |
| Email Address: |  |

|  |  |
| --- | --- |
| Secondary Contact Name: |  |
| Contact Title: |  |
| Phone Number: |  |
| Email Address: |  |

|  |  |
| --- | --- |
| DTI Contact Name: |  |
| Contact Title: |  |
| Phone Number: |  |
| Email Address: |  |

**Note: Primary contact will be responsible for the overall process of accepting payment cards at this location.**

1. **Merchant Business Operations:**

Please provide a brief description of your payment card process, describing how and in what capacity your process involves transmitting and/or storing cardholder data:

*Your answer here…*

Have your payment card processes changed over the last year?

Yes  No

If Yes, please explain:

*Your answer here…*

1. **Payment Acceptance Methods (check all that apply):**

|  |  |  |
| --- | --- | --- |
| **Method** | **Accepted** | **Details** |
| **IN-PERSON:**  Do you accept card present transactions?  If yes, please explain the process, including any forms used, participation by staff (e.g., swiping, entering into system), and equipment used (e.g., separate computer, payment card device, normal workstation). |  |  |
| **ECOMMERCE:**  Do you accept online payments?  If yes, what is the URL for your website (where the payment process starts)? |  |  |
| **PHONE:**  Do you accept payments over the telephone?  If yes, please explain the process including any forms used, participation by staff (e.g., swiping, entering into system), equipment used (e.g., separate computer, payment card device, normal workstation), and what type of connection (analog/cellular vs. IP). |  |  |
| **FAX:** Do you accept payments via fax?  If yes, explain how those are handled, where the fax machine is located, any security around the machine and/or location, staff involved, and machine type (e.g., plain paper fax or multi-function printer, analog based or IP/Network). |  |  |

|  |  |  |
| --- | --- | --- |
| **MAIL:**  Do you accept payments that come in via the U.S. Post Office?  If yes, please explain the process for handling those documents, who has access to them, and where they are stored before, during and after the payments are processed. Include details about securing and storing the forms. |  |  |
| **EMAIL:**  Do you accept payments via email?  If so, you must stop this practice immediately, as it is specifically forbidden by the PCI Council. Please speak with the PCI Team at OST to learn how to handle these situations. |  |  |

1. **ECOMMERCE: If you do not accept ecommerce or online payments, skip to section 6**.

Website URL/link where payment information is entered:

*Your answer here…*

Provide a brief description of what the ecommerce link is used for.

*Your answer here…*

Website URL where customer starts the process (if different than above):

*Your answer here…*

Please provide a brief description of the website and payment process:

*(e.g., customer goes to* www.yoursalespage.gov/*, selects services, enters contact information, then clicks Pay Now and is directed to the payment page.)*

*Your answer here…*

Are credit cards entered on behalf of customers?

Yes No If yes, please explain:

Is this link shared via email?

Yes No If yes, please explain:

Is this link shared via paper form?

Yes No If yes, please explain:

Is this link shared via electronic form?

Yes No If yes, please explain:

Is this link shared via text?

Yes No If yes, please explain:

Is this link shared via social media?

Yes No If yes, please explain:

Is this link posted on any other websites?

Yes No If yes, please explain:

Who hosts the web page?

Third Party

Department

IT

Don’t know

Other:

Please provide IT contacts that manage the ecommerce website (if known):

*Your answer here…*

1. **THIRD-PARTY SERVICE PROVIDERS:**

*A key component of PCI compliance is ensuring any third parties involved in the payment process are compliant. This includes third parties that host an ecommerce website, redirect to another third-party payment page, etc.*

Are there any third parties involved in any aspect of the payment card process for your merchant area?

Yes No

If yes, list any involved service providers (vendors), including a description of the service(s) provided. ***e.g., Lunch-Works, Deluxe, Flowbird, etc. … with a description.***

*Your answer here…*

Do you have a written agreement that indicates the service provider (vendor) is responsible for the security of cardholder data?

Yes No If yes, please explain:

Has the contract/agreement been reviewed and approved by our Legal Department?

Yes No If yes, please explain:

Has the contract/agreement been reviewed and approved by Information Technology?

Yes No If yes, please explain:

Do you have a program in place to review and validate any service provider's PCI-DSS compliance status before engaging in a new relationship?

Yes No If yes, please explain:

Do you validate the service provider’s (vendor’s) PCI-DSS compliance status at least annually by obtaining an updated Attestation of Compliance from the vendor?

Yes No If yes, please explain:

1. **PROCEDURES:**

Do written departmental payment card procedures exist?

Yes No If no, please explain:

Are staff aware of and trained on departmental procedures?

Yes No If no, please explain:

Do staff sign an annual policy acknowledgement?

Yes No If no, please explain:

Do staff receive annual PCI awareness training?

Yes No If no, please explain:

Does your department have any stored cardholder information (on paper or electronic)?

Yes No If yes, please explain:

If payment card information is written down, is all information shredded immediately after the transaction is processed?

Yes No If no, please explain:

If your department has payment card device(s), are the devices inspected for tampering and/or substitution according to procedure and inspections are logged?

Yes No If no, please explain:

Are devices kept in a secured and restricted area, away from public access?

Yes No If no, please explain:

Do you have the ability to process payment cards if normal modes of processing are down?

Yes No If yes, please explain:

1. **EMPLOYEE ATTESTATION STATEMENT**

I attest that the information in this merchant questionnaire has been completed to the best of my knowledge and belief. I understand the intent of this merchant questionnaire and that the information I have provided is an important element of the [*Entity Name here*] [Payment Card Handling Policy](https://treasurer.delaware.gov/wp-content/uploads/sites/55/2020/10/Statewide-Bank-Card-Acceptance-Policy-Oct-2019.pdf)*.*

|  |  |  |  |
| --- | --- | --- | --- |
| *Authorized Signature:* |  | *Date:* |  |
|  |  |  |  |
| *Printed Name:* |  | *Telephone #:* |  |
|  |  |  |  |
| *Title:* |  | *Location:* |  |

1. **ADDITIONAL MERCHANT MID INFORMATION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Merchant DBA** | **FSF XREF** | **MID** | **PROCESSING TYPE** | **SAQ TYPE** |
| ***Office of the State Treasurer*** | ***77 # for ACH or***  ***70 # for Credit Card*** | ***Starts with 526 #,***  ***345 #, or 372 #*** | ***In – Person, Online, or ACH*** | ***P2PE, A, D, and/or C*** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

***EQUIPMENT***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **HOST TERMINAL TYPE (POINT OF SALE)/ VIRTUAL TERMINAL** | **SERIAL NUMBER** | **HARD WIRED/ WIRELESS CONNECTION** | **IP ADDRESS(ES)** | **LOCATION** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |