|  |  |
| --- | --- |
| logo | **Longwood University** |

**Annual Credit Card Merchant Assessment**

|  |  |  |  |
| --- | --- | --- | --- |
| Merchant Name |  | Date |  |
| Merchant Fiscal Contact |  | Phone Number |  |
| Merchant Number(s) |  | | |
| Credit Card Brands Accepted | Visa  MasterCard  American Express  Discover | | |
| SAQ Level |  | Last Attestation Date |  |

|  |  |  |
| --- | --- | --- |
| 1 | By what method(s) do you accept credit cards? | In person Mail Fax Phone Email  Online Other |
| 2 | If you accept credit cards **in person**, do you have a point-of-sale (POS) terminal to accept credit card payments? | Yes – POS terminal connected to internet  Yes – POS dial-out terminal via analog phone line  N/A |
| 2.1 | Is the credit card number truncated on both the customer’s and merchant’s printed receipt? (last four recommended) | Yes No |
| 2.2 | Who is responsible for daily batch settlement? | Name:  Title: |
| 2.3 | What type of information is available on the daily batch settlement printed from the POS terminal? | Itemized sales by customer with full 16 digit credit card number listed  Itemized sales by customer but credit card number is not listed or is truncated  Summarized sales for the batch but sales are not itemized by credit card number/customer  Other |
| 2.4 | Where is the daily batch settlement and merchant copy of receipts stored? | Unlocked filing cabinet/desk  Locked filing cabinet/desk  Other, specify: |
| 3 | If you accept credit cards **in person** through a **swipe device**, please provide: | Manufacturer:  Model Number: |
| 4 | Is credit card data entered via computer terminal into a 3rd party website on behalf of the consumer? | Yes No |
| 4.1 | If yes, please provide: | Terminal Type:  Longwood Tag Number: |
| 4.2 | Is the computer terminal connected to any other system? | Yes No |
| 4.3 | Is credit card data entered ONLY via a secured terminal identified with a “***PCI Secure Workstation***” sticker? | Yes No |
| 4.4 | If your terminal is connected via the **internet** to a 3rd party who processes the credit card sale, have you confirmed they are PCI DSS compliant?  Provide the name of the 3rd party. | Yes No |
| 5 | If your department accepts credit cards **online**, what is the web address? | Web Address: N/A |
| 6 | Do you use a hosted solution where the customer is passed to a 3rd party to enter credit card information?  If yes, provide the name of the 3rd party. | Yes No |
| 7 | Do customers enter their credit card information on an LU domain and then get passed to a 3rd party for authorization? | Yes No |
| 8 | Are you interested in learning about the University’s hosted solution for accepting credit cards online? | Yes No Already Using |
| 9 | If you receive cardholder data via **fax**, is the fax machine in a secured area and are faxed documents destroyed immediately after the transaction is processed? | Yes No N/A |
| 10 | For transactions executed over the **phone**, please provide a copy of the form used to collect credit card data. | N/A |
| 11 | Do you process credit card information left on a voice message? | Yes No |
| 12 | If cardholder data is received through **email**, is the transaction processed? | Yes No |
| 13 | If you utilize a 3rd party service provider to transmit, store or process credit card information, have you confirmed them to be compliant with PCI DSS? | Yes No  University preferred solution |
| 13.1 | Please provide a list of all service providers and **proof of PCI compliance**. |  |
| 14 | Do you have any kiosks? | Yes No |
| 15 | Is credit card data stored on a Longwood device or system, or on Longwood premises?  If yes, explain. | Yes No |
| 16 | Do you store or retain any reports, receipts or written documentation with credit card numbers? | Yes No |
| 16.1 | If yes, do reports or receipts contain the full 16 digit credit card number? | Yes No |
| 16.2 | If yes, where is documentation stored? | Unlocked filing cabinet/desk  Locked filing cabinet/desk or safe  Other, specify: |
| 16.3 | If yes, how long do you store documentation? | Less than 1 year 3 years  Current Fiscal Year > 3 years  2 years |
| 17 | Do you destroy documentation immediately after authorization? | Yes No N/A |
| 17.1 | Explain how documentation is destroyed. | Mark-through  Shred  Cross-cut shred |
| 18 | Do you electronically store credit card data? | Yes No |
| 18.1 | If yes, where/how is credit card data electronically stored? | Departmental Server Other, specify:  Personal Computer |
| 18.2 | What type of credit card data is stored? | Credit Card Number Card Expiration Date  Magnetic Stripe Data Card Validation Code  Other, specify: |
| 19 | Are appropriate controls in place to limit physical access to systems and devices in the cardholder data environment? | Yes No |
| 20 | Are all media (electronic or paper) containing cardholder data kept in a secure and restricted area, away from public access? | Yes No N/A |
| 21 | Is a unique password assigned to each person with access to payment card processing? | Yes No N/A |
| 21.1 | What are the password change requirements?  (PCI states 90 days) |  |
| 22 | Is access restricted to paper and electronic media with credit card numbers and to systems that collect, store or process credit card information to only those individuals whose jobs require such access? | Yes No N/A |
| 23 | Do you send receipts and other documentation with full credit card numbers to offsite storage?  If yes, how long is it stored? | Yes No |
| 24 | Do you have written credit card handling procedures, to include data retention and disposal procedures (if applicable)?  **If yes, attach a copy**. | Yes No |
| 25 | Are you familiar with the University’s Payment Card Security Policy #1015 and applicable procedures? | Yes  No |
| 26 | Are you familiar with the University’s Funds Handling and Deposit Policy #4305? | Yes No |
| 27 | Do you keep the Director of Cashiering & Student Accounts aware of changes in your payment card program? | Yes No |
| 28 | Do you have a security awareness training program on the importance of cardholder data security for employees involved with credit card sales? | Yes No |
| 29 | If yes, how frequently is it offered?  **Provide documentation** verifying that all individuals involved in credit card activities receive training.  (Should be offered at least annually, and must be documented to be valid.) | Annually New hire |
| 30 | Do you require employees to acknowledge, at least annually, that they have read and understand Longwood policies/procedures on payment card processing?  If yes, please provide copies of ***Payment Card Security and Confidentiality Agreement***. | Yes No |
| 31 | Are you familiar with University Policy 6131 – Security Awareness and Training? | Yes No |
| 32 | Are you familiar with the following Information Security policies?  6104 – Acceptable Use of Information Technology Resources and Systems  6105 – Access to Information Technology Resources and Systems  6119 – Password Management  6127 – Physical Access  6132 – Incident Response | Yes No |

Merchant Fiscal Contact Signature

Reviewed By Date

**Notes:**