

**Departmental Procedures (TEMPLATE)**

**– For Processing through Preferred Third Party Hosted Solution and/or**

**Standalone Dial-up Terminal**

**Processing Payment Cards and Handling Cardholder Data**

|  |  |  |  |
| --- | --- | --- | --- |
| Merchant Name: |  | Date: |  |
| Merchant Fiscal Contact: |  | Merchant SAQ: | A  B |
| Credit Card Brands Accepted: | Visa  MasterCard  American Express  Discover | | |
| Method by which merchant  accepts credit cards: | In person  Via Mail  Fax  Phone  Online | | |
| Service Provider(s): | Nelnet Business Solutions  CASHNet  Elavon  Vantiv  (Commerce Manager) (E-Market) (Acquirer) (Acquirer) | | |

In order to comply with the PCI DSS and University Policy 3610 Procedure No. 3, departments/merchants who accept payment cards are required to develop and maintain a written set of policies and procedures that are consistent with university policy and which cover the process by which payment cards are accepted and credit card data is processed. The procedures should include but not be limited to:

* Segregation of Duties
* Physical Security and Identification of Card Processing Area
* Disposal
* Storage
* Personnel Screening and Criminal Conviction Check Procedures
* Information Technology Security
* Incident Response Plan

These procedures are to be submitted to the Bursar’s Office for approval and will be annually reviewed to ensure the written procedures match the department’s processes.

**Note**: The procedures contained in this example are procedures derived from the PCI requirements themselves. Departments who are developing their own written procedures may amend these procedures to match their specific business processes.

**I. Protecting/Handling Data**

* We do not store any cardholder data in an electronic format. **Pol. 3610 No. 1**
* Data that is not absolutely necessary in order to conduct business will not be retained in any format. **PCI 3**
* We do not store the full contents of the magnetic stripe under any circumstances. **PCI 3**
* We will not accept, request or retain such data via e-mail, voicemail or other “end-user technologies” electronic means. **Pol. 3610 No. 5**
* We will store cardholder data only long enough to complete the transaction. When we complete the transaction, we will destroy the cardholder data using an approved destruction method (see glossary). **Pol. 3610 No. 6**
* We will restrict access to system components to only those individuals who require access in order to perform their job duties. **PCI 7.1**

**II. Employee Background Checks**

* Prior to hiring, we submit all applicants to a criminal conviction background check. This includes university employees who were previously hired and who are applying for a position with the merchant. Employees who did not submit to a background check for whatever reason prior to their employment with the merchant will submit to one. Their duties involving the processing, transmitting and storage of cardholder data will be suspended until the background check is complete.

“Employees” defined in this requirement include full-time employees, part-time employees, seasonal employees, wage employees, and contractors and consultants who are directly involved in the processing, transmitting and storage of cardholder data and/or inhabit the card data environment.

* Applicants will be asked to disclose any criminal convictions as part of the application/interview process. All positions will be advertised with the notice: “**Employment will require a criminal background check**.”
* If the criminal conviction background check shows convictions the applicant revealed, the hiring supervisor will coordinate with the Bursar and Human Resources whether or not to confirm or withdraw the applicant’s offer of employment. A criminal conviction appearing in the background check does not automatically disqualify the applicant from employment with the university. The hiring supervisor will consider the nature of the conviction, the frequency, the relationship that a conviction has to the duties and responsibilities to the position to which the applicant is applying. The applicant may be asked by the hiring supervisor to provide additional details relating to the conviction.

If the criminal conviction background check shows convictions the applicant did not reveal, the hiring supervisor will be notified by the Human Resource Office and should immediately withdraw the offer of employment and so inform the applicant.

If an offer of employment is withdrawn based on the findings in the criminal conviction background check, the applicant or employee will have three days to respond. They may submit a rebuttal in writing explaining their conviction and why they feel they should be allowed to work for the department. They should explain any extenuating circumstances surrounding the convictions. The written rebuttal will be reviewed by an individual one level above the hiring supervisor. This individual will review the rebuttal, consult with the hiring supervisor and make a final decision. If the rebuttal is successful, the applicant will be hired and so informed. If the decision is to affirm the decision of the hiring supervisor, the applicant will be so informed and the offer withdrawn.

**Pol. 3610 No. 5**

**III. Training**

* Our department employees involved in processing, storing, and transmitting payment card transactions will complete annually and upon hire Payment Card Training offered through the Bursar’s Office. They will sign (upon completion) a Payment Card Security Agreement confirming their understanding and adherence to this policy. **Pol. 3610 No. 7**

**IV. Assessment**

* In order to verify our compliance with the PCI DSS, we will complete an annual Self-Assessment Questionnaire (SAQ) and on-site assessment conducted by the University’s E-commerce Manager. **Pol. 3610 No.8**
* We will complete an SAQ when our business process for accepting payment cards changes. **Pol. 3610 No.8**

**V. Protect Cardholder Data**

* Any primary account numbers (PAN) and sensitive authentication data is securely maintained and destroyed once the transaction is authorized. **PCI 3.2**
* We do not send or receive PANs via end-user technology (e.g., email, text, IM) under any circumstances. **PCI 4.2**
* If we received an unauthorized or unrequested PAN/Cardholder Data via:

A. Email (or any other end-user technology) – The transaction will not be processed. We redact the sensitive data and inform the sender that we cannot process information sent via email.

B. Voicemail – The transaction will not be processed. We delete the phone message; we then inform the sender that we cannot accept the information via phone message.

C. Fax/Mail – We ensure the sensitive authentication data is made unrecoverable through approved destruction method after the transaction is authorized. Incoming fax and mail is secured.

* We do not store the full contents of any track from the magnetic stripe under any circumstances even if it is encrypted. We only use the full contents of the stripe to authorize a transaction. **PCI 3.2.1**
* We will not store any card-validation code (i.e. the three or four digit code) used to validate a card-not-present transaction, personal identification number (PIN) or encrypted block after authorization. **PCI 3.2.2**
* Account numbers are masked if and when they are ever displayed (the maximum numbers that can be displayed are the first six and last four). Only employees with a business need may view the full PAN. **PCI 3.3**

**VI. Restrict Access to Cardholder Data by a Business Need to Know**

* We will restrict access to system components to only those individuals who require access in order to perform their job duties. **PCI 7.1**
* Our IT staff restricts access to our systems to the least privileges necessary for users to complete their job duties. **PCI 7.1.1**
* We assign privileges to our staff based on their job function. The Business Manager is granted access to view full transaction details. Our POS staff sees only merchant receipts. **PCI 7.1.2, 7.1.3**

**VII. Build and Maintain a Secure Network and Systems**

* IT staff update all vendor-supplied default settings and remove/disable default accounts prior to installing a system on the network. Applicable if you are hosting your own web server, point-of-sale terminals and/or payment applications. **PCI 2.1**

**VIII. Implement Strong Access Control Measures**

* We will complete and submit an access request form for each employee whose job duties necessitate the ability to view payment activity in Commerce Manager or CASHNet. Upon termination or a change in an employee’s position, which no longer requires access, we will notify the Bursar’s Office to revoke access to the aforementioned systems. **PCI 8.1.1, 8.1.3**
* Departmental IT staff have a unique, assigned ID to access system components, i.e. web server, payment systems. Access to system components is terminated immediately when an employee changes/leaves their position. **PCI 8.1.1, 8.1.3**
* In addition to Bursar assigned unique login ID credentials, departmental reporters will create their own password to authenticate into Commerce Manager. CASHNet reporters will gain access through Hokie SPA and two-factor authentication. **PCI 8.2, 8.2.3**
* We will not share our login/password credentials or create a departmental group, shared account toaccess Commerce Manager, CASHNet or third party payment applications. **PCI 8.5**

**IX. Restrict Physical Access to Cardholder Data**

* We physically secure all media. **PCI** **9.5**
* Media (all paper and electronic media containing cardholder data) that is to be distributed internally or externally is marked by our mail clerk with a stamp in red letters that reads “CLASSIFIED” on the envelope face before it is mailed. **PCI 9.6.1**
* If external media or a courier is used to transmit or transfer such data, we will use means that enable tracking of the data. Any transfer using these or similar means will be approved by appropriate levels of management before the fact. **PCI 9.6.2**
* When we distribute media externally, we receive approval from the Business Manager. The approval is recorded in a log that is maintained by the mail clerk. **PCI 9.6.3**
* We will limit physical access to cardholder data only to individuals who have a business need to know. Stored records are kept locked in our filing cabinet. Only authorized employees will possess a key. **PCI 9.5, 9.7**
* If we store media as part of our business process, it is stored only until the transaction is authorized. A copy of the phone or mail order form used by the department is attached. **PCI 9.8**
* Once media is no longer required for business use (after the transaction is authorized), we destroy it immediately using an approved destruction method, or we place it in a secured container located in our office that bears the label: “to-be-shredded.” **PCI 9.8**

**X. Protect Point-Of-Sale Devices**

* The Office of the University Bursar maintains a complete list of the inventory for POS devices. We maintain a list of POS devices at all merchant location(s) that includes the manufacturer, model number, serial number, Virginia Tech tag number, and the location of the devices. We update the list when devices are added, relocated, decommissioned, etc. **PCI 9.9, 9.9.1**
* The device list is up-to-date and reviewed at least semi-annually. **PCI 9.9.1**
* We conduct inventory check on the devices at least semi-annually and document the personnel and the results of the inventory check. **PCI 9.9**
* We inspect POS devices for tampering and substitution at least semi-annually. We check for addition of card skimmers to devices, manufacturer, model number, serial number, Virginia Tech tag number, and the location of the devices. **PCI 9.9.2**
* We verify with the Office of the University Bursar the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. **PCI 9.9.3**
* We do not install, replace, or return devices without verification with the Office of the University Bursar. **PCI 9.9.3**
* Employees who are at POS locations receive annual training to be aware of attempted tampering or replacement of devices as well as the procedures to detect and report any suspicious behaviors. **PCI 9.9.3**
* POS devices are secured after operating hours beyond public and/or non-authorized employee access.
* Any suspicious behavior is reported to the Office of the University Bursar and the University Police immediately, following the procedures under the University’s Payment Card Security Incident Response Plan.

**XI. Maintain a Security Policy**

* The university (Virginia Tech) has adopted information security policies covering the security of nonpublic personal financial information and use of university resources (see University Policy series 7000). These policies are updated as necessary to reflect changes in the university environment. We, (the merchant/department) abide by and operate under these policies. **PCI 12.5**
* The policies adopted herein are provided to every employee, contractor, consultant or any other party who has access to our (merchant’s) cardholder data environment. **PCI 12.1**
* The policies and procedures adopted herein are reviewed annually. They are updated to reflect changes in business processes. **PCI 12.1.1**
* As a university department, we adopt the university’s acceptable use policy contained in Policy No. 7000. It delineates how approved technologies may be appropriately used. In addition to the university acceptable use policy, critical technologies, such as remote-access technologies, wireless, laptops, tablets, e-mail and Internet usage is prohibited in the card data environment. This means that none of these technologies may be used to store, process, or transmit cardholder data. **PCI 12.3**
* Our security policy and procedures define the information security responsibilities for all personnel. **PCI 12.4**
* In the event of a security breach/incident, we follow the procedures outlined in the University’s Payment Card Security Incident Response Plan. We have formally assigned all duties and responsibilities regarding the reporting of such an incident to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. This individual is responsible for establishing, documenting, and distributing security response and escalation procedures to ensure timely and effective handling of all situations. **PCI 12.5.3**
* The departmental security awareness program is as follows: Payment Card Training for employees to be completed upon hire and annually thereafter covering security and proper handling/processing of cardholder data; completion and signature of the Payment Card Security and Confidentiality Agreement, a record of which will be maintained by the merchant; completion of the annual PCI SAQ; and annual review of the merchant’s departmental policies and procedures by the Office of the University Bursar. **PCI 12.6**

**XII. Procedures Performed Centrally by the Bursar’s Office for Departments Using the Preferred Third Party Hosted Solution**

* The third party service provider is responsible for the secure handling of cardholder data in accordance with the PCI DSS. As such:
* The Office of the University Bursar (OUB) has identified and maintained a list of the service providers with whom they have a contract. The OUB has also identified what services the service providers will perform for the university through the OUB and what aspects of their operations need to be PCI compliant. **PCI 12.8.1**
* The OUB will maintain a written agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data that they possess or otherwise store, process, or transmit on behalf of the university merchants, or to the extent that they could impact the security of the university’s cardholder data environment. The written agreement between the service provider and the OUB is included in the contract they sign when the service provider is engaged by the university. It includes the responsibilities of the service provider for the security of cardholder data it possesses relating to the processing, transmitting and storage of that data. The agreement states that the service provider is PCI compliant and will take the necessary steps to remain PCI compliant by validating its compliance annually. The agreement states that the service provider will notify the OUB if they are no longer PCI compliant. The service provider will take the necessary steps to become PCI compliant and so inform the OUB. They will inform the OUB of these steps in a timely fashion. **PCI 12.8.2**
* The OUB has an established process for engaging a new preferred third party service provider, including proper due diligence. Before engaging a service provider, the OUB will meet with a QSA to assess the service provider’s card data environment. They will review documentation such as flowcharts, Attestation of Compliance (AOC), vulnerability scans and any other information which will assist their decision making process. They will perform an audit of the service provider’s card data environment if their initial assessment is unsatisfactory. **PCI 12.8.3**
* The OUB will maintain a program designed to monitor service providers’ PCI DSS compliance status. The OUB will obtain the service provider’s annual AOC and quarterly Attestation of Scan Compliance (AOSC). In addition, some service providers have registered on Visa’s Global Registry of Service Providers. The OUB will monitor service providers’ PCI compliance status through a quarterly verification on Visa’s Service Provider Registry. The OUB will enlist the services of an Approved Scanning Vendor (ASV) to provide quarterly vulnerability scans and will provide the OUB with the scan results. **PCI 12.8.4**
* The OUB in partnership with the Information Technology Security Office (ITSO) has developed and disseminated an incident response plan for university merchants to follow in the event of a payment card breach.  **PCI 12.10.1**

**Glossary**

|  |  |
| --- | --- |
| **Approved Destruction Method** | Cross-cut shredding, pulp, or incinerate. |
| **Cardholder Data** | At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. |
| **Criminal Conviction Background Check** | Verifying that the applicant or the employee has no undisclosed criminal history in every jurisdiction where the applicants resides or has resided. The hiring manager and the OUB will review any convictions returned in the background check. Considering all application information, they will reach a consensus and so inform the applicant. |
| **Electronic format** | Data that is stored digitized. Examples include CD-ROM, DVD, USB flash drives, removable hard drives, email, internet, and intranet. |
| **Magnetic-Stripe Data** | Also referred to as “track data.” Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe. |
| **Media** | Any and all paper and electronic media containing cardholder data. |
| **Merchant** | For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers. |
| **PAN** | Acronym for “primary account number” and referred to as “account number.” It is the unique payment card number (typically for credit and debit cards) that identifies the issuer and the particular cardholder account. |
| **PCI DSS** | The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS is comprised of a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to mitigate risks. |
| **Sensitive Authentication Data** | Security-related information (including but not limited to card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. |
| **Service Provider** | Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded. |