Category 1 **<Merchant Name>** Operational Policies & Procedures

**<Merchant Name>** PCI DSS 4.0 merchant policy details the minimum requirements that **<Merchant Name>** will adhere to for securing payments received and processed on an outsourced e-commerce website. **<Merchant Name>** Operational Policy details who is responsible for each PCI DSS 4.0 policy and how that policy is being enforced.

|  |  |  |
| --- | --- | --- |
| **Revision History** | | |
| **Changes** | **Approving Manager** | **Date** |
| Initial publication |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Data Flow Policy**

Payment can only be processed in these approved ways: *<below are typical data flows and are to be used as a template and can be deleted, modified, etc. to fit your business practices>*

1. Outsourced E-commerce **(DATA FLOW MUST CONTAIN THE URL INFORMATION SHOWING THE REDIRECTION FROM YOUR HOSTED WEBSITE OR OUTSOURCED WEBSITE TO THE PAYMENT PROCESSOR URL FOR PAYMENT).**
2. Also you must complete the [**Data Flow Diagram**](https://sharepoint.umsystem.edu/sites/uminfopoint/media/_layouts/15/WopiFrame.aspx?sourcedoc=%7b3776778A-FB38-46D8-BB2B-19EA80DAC86F%7d&file=SAQ_A_Cardholder_Data_Flow_Diagram.docx&action=default)
   1. Customer goes form your university website to a 3rd party website (like TouchNet Marketplace).
   2. Once on the 3rd party website the customer fills their shopping cart.
   3. Customer clicks “proceed to payment” button.
   4. Customer is re-directed to the gateway (Possibly Touchnet the gateway) for payment information.   
      Credit card data is encrypted and sent to the payment processor.
   5. Authorization is returned back to the gateway.
   6. Customer is redirected back to the receipt page.

Payments can NEVER be accepted in the following ways:

1. Email
2. Other

Procedure to follow if you receive customer credit card data in an unapproved channel.

1. Email
   1. Write down the customer contact information
   2. Delete the email and empty your trash can in outlook
   3. Contact the customer explaining that their email has been deleted and that you cannot accept their payment by email. Let them know that you can accept payment by **<list your acceptance channels>**. Explain you are following policy to protect their personal information. Follow your procedures for accepting payments above and process their payment using an approved acceptance channel.
2. Other
   1. Write down customer contact information
   2. Destroy the card data that was received in an unapproved acceptance channel.
   3. Contact the customer explaining that their email has been deleted and that you cannot accept their payment by email. Let them know that you can accept payment by **<list your acceptance channels>**. Explain you are following policy to protect their personal information. Follow your procedures for accepting payments above and process their payment using an approved acceptance channel.

**Refund Policy**

Refunds should be submitted back to the same card that the original charge was processed. **<Individual A>** is the only person authorized to issue refunds. **<Individual A>** will verify the last 4 digits of the card with the customer and then process the appropriate refund amount back to the verified card. The refund is issued in the gateway.

**Cardholder Data Storage Policy**

All cardholder data storage policies and operational procedures are:

* Documented.
* kept up to date.
* in use.
* known to all affected parties.

**Paper storage policy for Pre-Authorization card data**

Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:

Paper Storage of card holder information at **<Merchant Name>** is kept **pre-authorization** per the following business reasons:

1. Reason X
2. Reason Y
3. Reason Z

Media such as paper storage and fax machines must be physically secured at all times.

1. **<Individual A>** is responsible for the security of the cardholder data that is stored on paper.
2. **<Individual A>** will lock the cardholder data stored on paper in a secure location (locked drawer, locked cabinet, etc.).
3. **<Individuals X, Y, & Z>** are granted access to the cardholder data stored on paper by **<Manager A>** since access is needed for their job duties.
4. **<Individual A>** must classify the sensitivity of all stored media so all individuals can determine the sensitivity of the data.

**Paper storage policy for Post-Authorization card data**

Paper storage of card holder information at **<Merchant Name>** is kept post-authorization per the following business reasons:

1. Reason X
2. Reason Y
3. Reason Z

**<Individual A>** is responsible for the security of the cardholder data that is stored on paper.

1. **<Individual A>** will lock the cardholder data stored on paper in a secure location (locked drawer, locked cabinet, etc.).
2. **<Individuals X, Y, & Z>** are granted access to the cardholder data stored on paper by **<Manager A>** since access is needed for their job duties.
3. **<Individual A>** must classify the sensitivity of all stored media so all individuals can determine the sensitivity of the data.
4. **<Individual A>** must keep an inventory log of all cardholder data stored on paper and the inventory log must be reviewed at least annually.
5. **<Individual A>** is responsible for updating the inventory each time a new record is filed, or an existing record is destroyed.
6. **<Individual A>** is responsible for media that is sent by secured courier or other delivery method that can be accurately tracked.
7. **<Individual A>** will obtain management approval from **<Manager A>** before data is moved or transferred, including when media is distributed to individuals.

* Note: The card verification code (CVV) cannot be retained upon completion of the authorization process.

**Data Retention and Disposal Policies**

Storage of account data is kept to a minimum.

Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:

1. Coverage for all locations of stored account data
2. Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization.
   1. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.
3. **<Individual A>** will determine the data storage amount and retention time that is required for legal, regulatory, and/or business requirements.
4. Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
5. **<Individual A>** will follow defined processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
   1. The retention requirements for cardholder data are <\_\_\_\_\_\_\_> days.
6. A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable is performed by **<Individual A>.**

**Paper Destruction Policy**

Retention of cardholder data stored on paper must not exceed **<X units>**. Once the retention period has been reached the cardholder data stored on paper must be destroyed. **<Individual A>** is responsible for the destruction or redaction of cardholder data that is no longer needed. Cardholder data can be destroyed or redacted by:

1. proper methods of destruction include:
   1. Cross Cut Shredding
   2. Incineration
   3. Pulping of the paper record
2. proper methods of redaction include:
   1. Removal of all but the last 4 of the customer credit card number (PAN) by hole punch
   2. Removal of all but the last 4 of the customer credit card number (PAN) by security marker or thick sharpie marker (if sharpie marker is used then the original with the card number blacked out will be copied, then the original will be destroyed, and the copy retained)
3. Materials are stored in secure storage containers prior to destruction.

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

**<Individual A>** is responsible for the following or they know who is responsible and **<individual A>** will follow-up to ensure the requirements are being met:

1. If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.
2. If the vendor default account(s) will not be used, the account is removed or disabled.

**Maintain a Vulnerability Management Policy**

**<Individual C>** is responsible for the University Webserver that manages how the customer gets to the gateway for payment:

1. Security vulnerabilities are identified and managed as follows:
   1. New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
   2. Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
   3. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
2. All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:
   1. Critical or high-security patches/updates are installed within one month of release.
3. All payment page scripts that are loaded and executed in the consumer’s browser are managed as follows:
   1. A method is implemented to confirm that each script is authorized.
   2. A method is implemented to assure the integrity of each script.
   3. An inventory of all scripts is maintained with written justification as to why each is necessary.
      1. This requirement applies to all scripts loaded from the entity’s environment and scripts loaded from third and fourth parties.
      2. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

**User Authentication Policy**

**<Individual A>** is responsible for the following or they know who is responsible and **<individual A>** will follow-up with **DoIT** or the **3rd party service provider** to ensure the requirements are being met:

1. User ID Policy
   1. All users are assigned a unique ID before allowing them to access system components or cardholder data.
   2. Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary, on an exception basis, and are managed as follows:
      1. Account use is prevented unless needed for an exceptional circumstance.
      2. Use is limited to the time needed for the exceptional circumstance.
      3. Business justification for use is documented.
      4. Use is explicitly approved by management.
      5. Individual user identity is confirmed before access to an account is granted.
      6. Every action taken is attributable to an individual user.
   3. Access for any terminated users is immediately deactivated or removed.
2. User Authentication policies:
   1. All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:
      1. Something you know, such as a password or passphrase.
      2. Something you have, such as a token device or smart card.
      3. Something you are, such as a biometric element.
   2. If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:
      1. Set to a unique value for first-time use and upon reset.
      2. Forced to be changed immediately after the first use.
   3. If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:
      1. A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
      2. Contain both numeric and alphabetic characters.
         1. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment. Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.
   4. Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.
   5. If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single factor authentication implementation) then either:
      1. Passwords/passphrases are changed at least once every 90 days,

OR

* + 1. The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.
       1. This requirement does not apply to service providers’ customer accounts but does apply to accounts for service provider personnel.

**Test Security of Systems and Networks Regularly**

**<Individual A>** is responsible for the following or they know who is responsible and **<individual A>** will follow-up with **DoIT** or the **3rd party service provider** to ensure the requirements are being met:

1. External vulnerability scans are performed as follows:
   1. At least once every three months.
   2. By a PCI SSC Approved Scanning Vendor (ASV).
   3. Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.
   4. Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.
2. External vulnerability scans are performed after any significant change as follows:
   1. Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.
   2. Rescans are conducted as needed.
   3. Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).
3. iFrame Payment Page Integrity
   1. A change- and tamper-detection mechanism is deployed as follows:
      1. To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.
      2. The mechanism is configured to evaluate the received HTTP header and payment page.
      3. The mechanism functions are performed as follows:
         1. At least once every seven days

OR

* + - 1. Periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).

**Security Policy**

The **Treasurer’s office** is responsible for an overall security policy. That is:

* Established
* Published
* Maintained
* Disseminated to all relevant personnel, as well as to relevant vendors and business partners.

All employees that come into contact with customer cardholder data at **<Merchant Name>** are responsible for protecting cardholder data.

**<Individual A>** is responsible for reviewing the merchant policies and procedures at least annually and polices must be updated if/when the environment changes.

**The UM System Incident Response Plan includes the following:**

1. Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
2. Incident response procedures with specific containment and mitigation activities for different types of incidents.
3. Business recovery and continuity procedures.
4. Data backup processes.
5. Analysis of legal requirements for reporting compromises.
6. Coverage and responses of all critical system components.
7. Reference or inclusion of incident response procedures from the payment brands.

**Merchant Incident Response Plan details the following:**

**<Individual A>** is responsible for establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.

**<Individuals X, Y, & Z>** are responsible for reporting any suspected data breaches to **<individual A>.** **<Individual A>** is responsible for gathering all relevant information and reporting any suspected data breaches to the [information security officer](https://www.umsystem.edu/ums/is/infosec/iso) at the respective campus or business unit. **<Individual A>** is responsible for meeting with the Information security officer not more than one week following the incident to review the results of the investigation to determine the root cause of the compromise and evaluate the effectiveness of the incident response plan.

**Security Training**

**<Individual B>** is responsible for the formal security awareness program to make all personnel aware of the cardholder data security policy and procedures. **<Individual B>** is responsible for all new hires and **<Individuals X, Y, & Z>. <Individual B>** will use the [new hires checklist](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/New_Hire_Checklist.docx?d=wfd390590756f482683e6ae590101e78a) to perform the following:

1. Have all relevant staff read, understand, and attest that they have read and understood the merchant specific policies and procedures.
2. Have all relevant staff read, understand, and attest that they have read and understand the University credit card policy (<https://www.umsystem.edu/ums/fa/treasurer/payment_card_policies>)
3. Have the new hire complete the [cardholder data processing agreement & annual training form](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Merchant_Request_Form.docx?d=w27f4e88c0e8e4029b6b9b75734b13ade)
4. Contact The Treasurer’s Office to have your new hire enrolled into the appropriate online training upon hire. New hires are enrolled at the beginning of each month.
   1. New hires must complete the online training upon hire and annually thereafter.
      * Regular staff go through [Percipio](https://umsystem.percipio.com/)
      * Hospital staff go through SABA
      * Students regardless of campus go through [Canvas](https://canvas.umsystem.edu/)
   2. **<Individual A>** will maintain a training log that lists who was enrolled and when they last completed the annual training.
5. Train the new hire with specific functional training as it relates to their job duties.
   1. For example, train them to use the specific terminal or point of sale device that they will be processing transactions on. This training should include the desk manual that you develop.

**Service Providers Policy**

**<Individual A>** is responsible for the following as it pertains to managing third party service providers:

1. Maintain a list of all service providers that **<Merchant Name>** account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.

|  |  |
| --- | --- |
| **Service Provider Name** | **Service(s) Performed** |
| **Example**: Chase Paymentech | Acquiring Bank and payment processor |
| **Example**: TouchNet | E-commerce Gateway |
| **Example**: Cintas | Document secure storage and destruction |
|  |  |
|  |  |

1. Written agreements with TPSPs are maintained as follows:
   1. Written agreements are maintained with all TPSPs (3rd party Service Providers) with which account data is shared or that could affect the security of the CDE (Card Holder Data Environment).
   2. Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity’s CDE.
2. **Office of the Treasurer** will complete [the 3rd party check list](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/3rd_Party_Checklist.docx?d=w1f1f7e4b799e4d28a56643a2c720dfb8) before a new 3rd party service provider is to be added to the cardholder data environment to ensure proper due diligence
3. The **Office of the Treasurer** monitors the TPSPs’ PCI DSS compliance status at least once every 12 months.
4. Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.
   1. A “Responsibility Matrix” should be given to **Office of the Treasurer** to satisfy this requirement.