Category P2PE **<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 using a P2PE (Point-to-point encrypting) validated solution. **<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 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Documented Data Flow**

Payments 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. In person swipe on the P2PE validated solution device.
	1. Card is physically swiped or dipped capturing the data on the magnetic stripe.
	2. Encrypted cardholder data is sent through the POS and through our network to the gateway of the P2PE validated solution.
	3. The payment is then sent on the payment processor.
	4. Authorization is returned back over the network.
	5. Customer signs the merchant receipt and the customer receipt is presented to the customer.
2. In person swipe fails (hand key payment)
	1. Card cannot be swiped or dipped so the PAN and expiration date has to be hand keyed into the P2PE validated solution device.
	2. Encrypted cardholder data is sent through the POS and through our network to the gateway of the P2PE validated solution.
	3. The payment is then sent on the payment processor.
	4. Authorization is returned back over the network.
	5. Customer signs the merchant receipt and the customer receipt is presented to the customer.
3. Phone payment
	1. Payment is taken over the phone via analog phone line or special cellular phone used just for taking card data over the phone.
	2. PAN and expiration date is hand keyed into the P2PE validated solution device.
	3. Encrypted cardholder data is sent through the POS and through our network to the gateway of the P2PE validated solution.
	4. The payment is then sent on the payment processor.
	5. Authorization is returned back over the network.

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 ask the customer for the full card number to process the refund back to the verified card. **<Individual A>** will hand key the card number and expiration date into the P2PE validated solution device and never write down the cardholder data on paper.

**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.

The card verification code is not 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.

**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.

**Terminal Physical Security**

**<Individual A>** is responsible for developing and maintaining a [Capture Device Inventory Log](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Capture_Device_Inventory_Log.docx?d=w01eea484fe174cd688f377c95f01128f). **<Individual A>** is responsible for making sure the inventory log has the following minimum requirements:

1. Make/Model of the terminal(s)
2. Location of the Terminal(s)
3. Serial number or unique identification number of the terminal(s)
4. Serial number(s) of the tamper tape that was added to the swipe devices.

**<Individual A>** is also responsible for maintaining the log so that it is updated anytime a new device is added, relocated, no longer in use, etc. If any device the merchant has is a cellular device and is mobile then a [Cellular Terminal Log](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Cellular_Terminal_Log.docx?d=w11e077796fad46218eded513fe4aa4a5) must be maintained by **<individual A>** detailing where the device is and who is in possession of it at all times.

**<Individual A>** is responsible for inspecting all terminals to look for tampering or substitution using the [Capture device Periodic Inspection Procedure](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Capture_Device_Periodic_Inspection_Procedure.docx?d=w491cec7229dd43c0b7ebcc1e797fb32a) every 3 months or if the terminals are open to the public then **DAILY**.

**<Individual A>** is responsible for training **<Individuals X, Y, & Z>** to be aware of attempted tampering or replacement of devices as follows:

1. **<Individuals X, Y, & Z>** Mustverify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
	1. Only the P2PE provider is authorized to access, modify, or trouble shot devices.
	2. **<Individual A>** will call P2PE provider to initiate the access.
2. **<Individuals X, Y, & Z>** willnot install, replace, or return devices without verification by **<Individual A>**.
3. **<Individuals X, Y, & Z>** will be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
4. **<Individuals X, Y, & Z>** will report suspicious behavior and indications of tampering or substitution to **<individual A>**.

The terminal physical security policies and operational procedures is documented, in use, and known to all affected parties.

**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**: TouchNet | P2PE solution Provider |
|  |  |
|  |  |

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.