

## CMU Merchant Sites Security Guidelines

All sites wishing to accept credit cards must go through Payroll and Travel Services.

All departments accepting credit card payments must designate one employee as the Merchant Account Manager.

Keep an updated list of employees who have access to credit card information. This includes databases, filing cabinets, offices, etc. A template can be found on the [Controller's website](#).

All employees involved in the processing of credit card transactions must read, understand and follow the Merchant Operating Guide as well as the CMU Merchant Sites Security Guidelines.

Duties within a department should be segregated so that one person does not perform processing from the beginning to the end of a process. For example, one employee should not be processing credit cards, recording the revenue and reconciling the accounts.

Access to cardholder data should be limited to only those individuals whose job requires such access.

Merchants must contact Payroll and Travel Services in the event that they will be making any changes to their method of processing after the merchant has been initially set up. Examples include changing from terminal based processing to processing through PC software, through a web site, terminals built into cash registers, touch tone phone authorization, or processing through a lock box. Payroll and Travel Services must approve all such changes.

If a Merchant no longer wishes to accept credit cards, the Merchant must contact Payroll and Travel Services.

Accept cardholder data by telephone, mail, or in person only, not through electronic mail.

You are prohibited from engaging in mail/telephone order transactions unless you indicated on your original Application/Sales Agreement that you accepted or planned to accept such transactions or you have received subsequent written approval to do so from Payroll and Travel Services.

All face-to-face transactions should have the payment card present and obtain a signature. Always verify that the card is valid and signed. Compare signatures and check for ID where possible and feasible.

When it is necessary to store cardholder data prior to processing the transaction, it must be stored in a "secure" environment. Secure environments include locked drawers, file cabinets, offices and safes.

All documentation containing cardholder data must be destroyed in a manner that will render them unreadable (cross-cut shredded, incinerated, or pulped) after the payment has been processed.

<p>Cardholder receipts generated from a point-of-sale terminal must include only the last four digits of the account number, replacing all preceding digits with fill characters that are neither blank spaces nor numeric characters, such as “x”, “*”, or “#”. The expiration date must be excluded.</p>
<p>Merchant receipts generated from a point-of-sale terminal must exclude the card expiration date and should only have the last 4 digits of the account number.</p>
<p>Transactions should be batched on a daily basis.</p>
<p>Merchants are required, in good faith, to maintain a fair policy for the exchange and return of merchandise and for resolving disputes over merchandise and/or services purchased with a payment card. If a transaction is for non-returnable, non-refundable merchandise, this must be indicated on all copies of the sales draft before the cardholder signs it. A copy of your return policy must be displayed in public view.</p>
<p>Merchants should not, under any circumstances, pay any card refund or adjustment to a cardholder in cash. If cash is refunded and the cardholder files a dispute your department will bear the loss of income from the transaction.</p>
<p>Retain the payment information from all transactions and any original, signed documentation in a secure location for a minimum of 3 years per record retention guidelines.</p>
<p>Wherever possible, storage areas should be protected against destruction or potential damage from physical hazards, like fire or floods.</p>
<p>Under no circumstances should cardholder information (full account number, type, expiration date, CVV2 (3 or 4 digit code), or track data) be entered and stored on any computer database in the department unless it is part of a secure system that has been approved by Payroll and Travel Services.</p>
<p>Under no circumstances should cardholder data be emailed.</p>
<p>Under no circumstances should cardholder data be mailed in interoffice mail.</p>
<p>Do not store the CVV2 (also known as the card-validation code/value or the 3 or 4 digit code) printed on the front or back of a payment card used to verify card-not-present transactions.</p> <p>Do not store the full content of any track from the magnetic stripe (that is on the back of the card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2 and magnetic stripe data.</p>
<p>Do not store the personal identification number (PIN) or the encrypted PIN block.</p>
<p>Cardholder data must remain in the department processing the transaction. This information should never be distributed to another department.</p>
<p>All cardholder data and payment information should be classified as confidential. If it is necessary to send payment information to a third party it should be done by a secured courier or</p>

other delivery method that can be accurately tracked.

Payroll and Travel Services must be contacted if you are disposing of any credit card processing equipment. This includes terminals and computers.

Credit card information includes the following...

**Cardholder data** - Primary Account Number, Expiration Date, CVV2 (3 or 4 digit code) and magnetic stripe data.

**Payment information** - Cardholder name, Transaction date, Last 4 digits of the credit card number, authorization code, card type and amount. Examples include receipts and batch reports.

\*The security guidelines will be reviewed and updated on a yearly basis or as needed.