The Financial Services, Payment Card Services Office administers the University Merchant process so that you have the capability of accepting payment cards. ASU has contracted with vendors to supply the University departments with Payment Card Industry Data Security Standard (PCI DSS) compliant options to accept payment cards online to sell goods, and services to its customers. With this service, the University merchants are subject to, and must understand and comply with all rules, regulations and contractual provisions regarding the handling of payment cards. The regulations include the Payment Card Industry Standards and the Card Associations (MC, VISA, AMEX, DISCOVER) merchant requirements.

The University merchants are required to comply with these regulations and requirements in order to continue to accept payment cards. In the event of non-compliance, the Financial Services Office reserves the right to revoke those privileges until which time compliance is achieved.

Non-compliance with the Payment Card Industry standards puts ASU at risk for:

- Large monetary fines assessed to your department and/or Arizona State University
- Loss of merchant status for your department
- Possible loss of merchant status for all of Arizona State University
- Loss of faith, by the community in the Arizona State University name

General Rules, Regulations, and Guidelines

A) Security

1. All ASU Merchants are required to review the Payment Card Industry Data Security Standard (PCI DSS) located online at https://www.pcisecuritystandards.org/.

2. If you process credit card data in any form (face-to-face or electronic), you need to be in compliance with Payment Card Industry Data Security Standards (PCI DSS).

3. All eCommerce gateways need to be PCI DSS certified and compliant with ASU’s security requirements.

4. All electronically captured information must be in an encrypted secure socket layer (SSL) that meets the PCI DSS requirements with minimum need-to-know basis access to cardholder information.
5. Any vendor technical documents provided to the Merchant must be kept in a secure location and not shared with anyone else without prior approval of the Financial Services, Payment Card Services Office.

6. To meet the Arizona Revised Statute (A.R.S) 44-7501 (Notification of Breach of Security System), the PCI-DSS payment card industry provisions and requirements, all suspected and/or confirmed security compromises need to be reported immediately to the University Information Security Officer and the Financial Services, Payment Card Services Office. If a breach has occurred with the data you are storing, you are responsible for any and all externally imposed fines as well as the costs associated with bringing your location into compliance.

7. It is prohibited to store card information and card-validation codes (three-digit value printed on the signature panel of a card) on any ASU computer, database or server. You must protect cardholder data by keeping it secure and confidential.

8. You must not collect card numbers and card information via e-mail, unsecured or network fax machines, or cell phones, as they are not secure formats.

9. You agree to maintain all card documentation containing card account numbers in a “secure” environment, restricting user access to payment card account numbers to a need-to-know basis. Secure environments include locked drawers, file cabinets in a locked office, and safes. Credit card receipts and card documentation needs to be treated in the same manner you would treat large sums of cash. Your department is responsible for any losses due to inadequate internal controls.

10. You need to keep all original copies, imaged copies or microfilmed copies of card documentation (registration forms, mail-in forms, internal documents) for no less than 180 days and no longer than two (2) years depending on the documentation being retained. After which time, cardholder data must be deleted or destroyed (i.e. shredded) before it is physically disposed.

11. You agree not to disclose or acquire any information concerning a cardholder’s account without the cardholders consent. You will not sell, purchase, provide, disclose or exchange card account information or any other transaction information.

12. Treat the following as high-risk transactions: use of anonymous e-mail address, shipping address from overseas, prisons, hospitals, or mail drops.
Approval: ______________________________________________
Agency/Org Manager Printed Name

Approval*: ______________________________________________
Agency/Org Manager Signature Date

* By signing this form the agency/org manager is approving the establishment of this merchant account and assumes responsibility for compliance with the Payment Card Industry Data Security Standards and University guidelines as outlined above and in the attached document.

➢ Please call Financial Services/Payment Card Services if you have any questions at 480-965-9823.
➢ Please complete and return original to:
  David Ketterman
  Student Business Services
  Campus Mail Code 0303

Financial Services, Payment Card Services recommends that all staff interacting with payment cards view the short PCI video at http://www.compass-com.com/moneris/pci/PCI_main.html.

Additional information on PCI DSS may be obtained by visiting the PCI Security Standards Council website at: https://www.pcisecuritystandards.org.