

**SAN DIEGO STATE UNIVERSITY RESEARCH FOUNDATION
CREDIT CARD PROCESSING & SECURITY POLICY
MERCHANT SERVICES POLICIES & PROCEDURES**

Last Revised: April 2020

POLICY STATEMENT

Introduction

Some San Diego State University Research Foundation (SDSURF) projects accept donations or payments for goods or services such as application and registration fees and have been set up with credit card merchant accounts. Projects accept payments through point of sale (POS) terminals or have agreements with third-party processors to provide payment gateway services that allow customers to make purchases on-line via the internet.

The ability to accept credit card payments comes with risk and the responsibility to protect sensitive cardholder data.

SDSURF projects that participate in card processing activities (merchants) are required to follow strict procedures to protect customers' credit card data. The credit card companies (including Visa, MasterCard, Discoverer, and American Express) have developed standards that all credit card merchants must follow called Payment Card Industry Data Security Standards (PCI DSS). In addition, all projects utilizing merchant accounts must also adhere to the ICSUAM Debit/Credit Card Payment Policy, San Diego State University Information Security Plan and the San Diego State University Research Foundation Merchant Services Policies and Procedures.

Failure of merchants to comply with these standards and guidelines and otherwise adequately protect sensitive cardholder information will result in the suspension of merchant privileges. In addition, fines may be imposed by the affected credit card company, ranging from \$5,000-\$50,000 per violation, per month out of compliance, per credit card company.

Program Requirements

All projects shall adhere to appropriate standards for credit card merchant services including training, outsourcing agreements with third-party providers, data and system security, PCI compliance, cost responsibility, and fiscal responsibility. The following program requirements are intended to ensure credit card payments made to SDSURF projects are processed in a secure manner, in compliance with industry PCI DSS standards, applicable federal and state legislation and CSU, SDSU and SDSURF policies and procedures.

1. All card processing activities of SDSURF projects will be conducted through merchant accounts obtained through the Merchant Account Acquisition Procedure. Merchant accounts will be issued only to particular SDSURF funds for a specific use. Accounts operated by parties other than the approved entity or for a purpose other than that approved may be rescinded without notice.

2. In no case should cardholder data be processed, stored or transmitted using any device on SDSU or SDSURF networks without explicit prior approval from the appropriate SDSU and SDSURF authorities.
3. Transactions must be completed on approved, secure, fully hosted third party payment processing services. Projects will not use the services of any bank, corporation, entity or person other than the third party that SDSURF has contracted with for authorization or processing of credit card transactions, unless otherwise approved by the SDSURF CFO, Controller, or Director of Accounting & Reporting.
4. All service providers must be approved by SDSURF in advance and must be certified PCI DSS compliant and certified by Visa and MasterCard to accept credit card transactions securely over the internet.
5. All application providers must be approved by SDSURF and/or SDSU in advance and must be certified as PPA-DSS (Payment Application Data Security Standards) compliant.
6. All third parties with access to cardholder data shall be required to contractually acknowledge responsibility for the security of cardholder data in their possession and be contractually required to adhere to PCI DSS compliance, including an annual validation of compliance through methods authorized by a PCI certified Quality Security Assessor. *See Appendix A for sample contract language.*
7. All card processing activities and payment technologies used by SDSURF projects must comply with the Payment Card Industry Data Security Standards (PCI DSS) and Payment Application Data Security Standards (PA-DSS). No activity or technology may obstruct compliance with the PCI DSS. All projects processing credit card transactions will participate in an annual PCI risk assessment.
8. All projects that receive or expect to receive credit card payments must also comply with the San Diego State University Information Security Plan and the SDSURF Merchant Services Policies & Procedures.
9. Projects may accept only those credit card brands authorized by SDSURF and agree to operate in accordance with the contract(s) SDSURF holds with its Service Provider(s) and Card Issuers. Project PIs/Project Directors are responsible for ensuring that all transactions are in compliance with third party operating guides and credit card processing contracts regarding security and privacy.
10. Exceptions to this policy may be granted only after a written request from the project has been reviewed and approved by the CFO, the Controller, or the Director of Accounting & Reporting.

Scope

This policy applies to all faculty, staff, students, organizations and individuals who, on behalf of SDSURF projects, handle electronic or paper documents associated with credit or debit card receipt transactions or accept payments in the form of credit or debit cards. The scope includes any credit or debit card activities conducted at all locations.

PROCEDURES

This manual explains policies, procedures, and best practices relative to the use of merchant card services. This manual informs everyone involved in payment card processes of their responsibility to establish and maintain proper internal controls ensuring responsible payment processing. Everyone involved with use, administration, and oversight of payment card transactions and processing is responsible for ensuring that periodic updates to this manual are reviewed.

Merchant Responsibilities:

PIs or Project Directors who accept credit card payments to their foundation funds are responsible for safeguarding the confidentiality of sensitive data and personal information relating to the sale or purchase of goods and services and for ensuring compliance with information privacy legislation and with University and Research Foundation policies on information privacy. Safeguards and responsibilities include, but are not limited to the following:

Protection of cardholder data

- Do not store credit card information (full account number, type, expiration date, track data, etc.) on any computer or electronic device (desktop, laptop, database, spreadsheet, images, USB drive, disk, network, pda, etc.).
- Do not transmit cardholder data via e-mail.
- Credit card information should not be faxed. Procedures for faxing payments must be reviewed and approved by the Director of Accounting and Reporting, the Controller, or CFO and the appropriate campus authority.
- Store only essential information. Avoid the retention of paper records containing complete credit card numbers. If, for business reasons, you must store full card numbers then do so for no longer than is required by the credit card companies. Mark these records as 'Confidential'.
- Transmissions of sensitive cardholder data must be encrypted through the use of SSL.
- Securely dispose of sensitive cardholder data when it is no longer needed.
- Do not store the full contents of any track from the magnetic stripe, the card-validation code (the three digit value printed on the signature panel of a card) or personal identification number, PIN, information in any manner.
- Mask all but the last four digits of the account number when displaying cardholder data.

Restricted access to cardholder data

- Restrict access to card account numbers to users on a need-to-know basis. Access must be limited to employees of SDSU or SDSURF who have a signed Confidentiality Agreement on file with the appropriate Human Resources department.
- Maintain an updated list of employees who have access to credit card information. The list should contain the following columns: Last Name, First Name, RedID, Position/Title, Cardholder Data Accessible, and Format. Include a brief justification linking access to the sensitive information to the employee's job.

- Protect cardholder data from unauthorized access. Physically secure paper records containing full or partial credit card numbers in locked cabinets or offices with adequate key control. Wherever possible, storage areas should be protected against destruction or potential damage from physical hazards, like fire or flood.
- Equipment and media containing cardholder data must be physically protected against unauthorized access.
- Cardholder data must be deleted or destroyed before it is physically disposed (e.g. by shredding paper, and degaussing media.)
- Proper procedures for the distribution and disposal of any media containing cardholder data must be followed.

Point of Sale (POS) Terminal Protections from Tampering and Substitution

San Diego State University Research Foundation and projects processing credit card transactions through swipe terminals are required to maintain an up-to-date inventory of all point of sale (POS) swipe terminals that capture payment card data. The projects will be responsible of protecting card present processing terminals from tampering or substitution.

- All point of sale (POS) terminals must be tracked and monitored on an ongoing basis to look for tampering or substitution (e.g., altered seals or screws, wiring, holes in the device, materials used to mask damage from tampering).
- A list must be maintained of all POS terminals that capture payment card data, for which the list is to include the following: Make, model, unique identifier, and location of device.
- Ensure that the list of terminals is updated when terminals are added, relocated, decommissioned.
- Physically secure all terminals that capture payment card data.
- Wireless credit card processing terminals must be stored securely in a locked area when not in use.
- Cashiers must perform a daily visual inspection of terminals that capture payment card data.

PIs/ Project Directors for programs approved as merchants shall ensure that all employees responsible for systems and procedures related to credit card transactions processed through POS terminals have completed an annual training on POS equipment tampering prevention and awareness.

- Verify the identity of any third-party claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
- Not install, replace or return devices without verification.
- Be aware of suspicious behavior around devices.
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel.

Training Responsibilities & Security Awareness

- PIs/Project Directors for programs approved as merchants shall ensure that all employees responsible for systems or procedures related to credit card transactions and cardholder data have completed mandated Security Awareness Training annually. To enroll in training, contact Deanna Vaughn, Merchant Services Coordinator at dmvaughn@sdsu.edu.
- PIs/Project Directors are responsible for providing necessary training to employees to ensure staff members adhere to policies and procedures related to credit card merchant services and information security.

Data and System Security

Cardholder data must not be processed or stored on any SDSU/SDSURF system without explicit approval. All systems must be secured and managed in compliance with the SDSU Information Security Plan.

Cost Responsibility

The project is responsible for all fees associated with use of a merchant account, including but not limited to equipment fees, supply costs, processing fees, dedicated phone lines and all costs related to maintaining PCI-DSS compliance. The project is also responsible for any fines and penalties resulting from noncompliance with PCI DSS standards, federal and state legislation, and University and Research Foundation policies. Fees will be assessed to the FOAP designated on the Merchant Site Request Form.

Fiscal Responsibility

Projects that provide credit card merchant services are responsible for adhering to internal control standards for the safeguarding of receipts and data, the proper deposit and posting of receipts, and the reconciliation of receipts.

PCI DSS Compliance

The PI/Project Director is responsible for compliance with PCI DSS standards. At least annually, the PI/Project Director must complete the appropriate PCI Security Standards Council Self-Assessment Questionnaire (SAQ) in its entirety, including the Attestation of Compliance. Completed forms should be submitted to the Merchant Services Coordinator, MC 1947.

If users are redirected to a third-party processing site from a project website then PCI DSS requires quarterly vulnerability scans by a PCI SSC Approved Scanning Vendor (ASV) for all externally-facing IP addresses. Evidence of a passing scan from the ASV must be attached to the PCI Security Standards Council Self-Assessment Questionnaire (SAQ). Scans will be coordinated by the SDSU Technology Security Officer.

Loss or Theft of Account Information – Incident Response

A merchant must immediately report to SDSURF and University the suspected or confirmed loss or theft of any material or records that contain cardholder data. Failure to immediately notify the proper authorities will put the merchant at risk of steep penalties for each incident. Merchants are subject to fines by each of the impacted credit card brands.

In the event that transaction data is accessed or retrieved by any unauthorized entity, notify the SDSURF CFO, the Controller, the Director of Accounting & Reporting or Merchant Services Coordinator immediately.

SDSURF will notify the merchant bank, card processor and SDSU ITSO to coordinate the incident response program.

Merchant Approval

Upon written approval and agreement with and adherence to published policies and procedures, San Diego State University Research Foundation (SDSURF) projects may accept VISA, MasterCard, Discoverer or American Express, and debit cards with a VISA or MasterCard logo as a form of payment for goods and services.

All projects interested in accepting credit card payments to Research Foundation funds, either via the web or in person using a terminal, must complete the Merchant Account Request Form and submit to the Merchant Services Coordinator in Finance & Accounting. The requestor must be a PI or Project Director with budget and signature authority on funds administered by SDSURF.

The Chief Financial Officer, the Controller, or the Director of Accounting & Reporting shall review and approve all credit card processing activities associated with SDSURF funds.

Merchants must contact Finance & Accounting 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 website, terminals built into cash registers, touch-tone phone authorization, or processing through a lock box. Finance & Accounting must approve all such changes.

Merchant Account Set-Up Requests – Card Swipe/Point of Sale (POS) Terminals

Payment Processing Service

SDSURF has an agreement with Elavon to provide merchant card payment processing services. All SDSURF projects should utilize Elavon. Projects may request an exemption from this requirement by providing a business case justifying an alternate vendor or process to the Merchant Services Coordinator in Finance & Accounting, MC 1947. Projects shall not enter into an outsourcing agreement with a third-party provider, including software applications for credit card processing, until the business case has been approved by the Director of Accounting & Reporting, the Controller, or the Chief Financial Officer.

Point of Sale Swipe Terminals

For non-internet transactions, a point of sale (POS) swipe terminal with printer and a dedicated phone line are required. Each merchant is responsible for the installation and cost of their dedicated phone line. The purchase price, programming fees and supply costs for terminals is billed directly to the merchant through their Elavon monthly invoice and charged to the RF fund identified on the Merchant Site Request Form.

All POS terminals must be PCI DSS compliant and be pre-approved by Elavon and SDSURF. Prior to replacing a POS terminal, contact the Merchant Services Coordinator to ensure that a qualified terminal is purchased.

Online Payment Gateway (Converge)

Elavon endorses the use of its online payment gateway “Converge” for internet POS services. The use of the application and configuration and maintenance of terminals must be compliant with the PCI Data Security Standard and its use must be approved by SDSURF and Elavon.

1. Complete a Merchant Account Request Form.
2. Submit completed form to the Merchant Services Coordinator, SDSURF Finance & Accounting, MC 1947.
3. The request form will be reviewed and the appropriate services determined.
4. Once approved, the information will be forwarded to Elavon, who will process the request and issue a merchant id number.
5. Elavon will mail a new merchant welcome kit and contact the merchant directly to walk designated project personnel through the process of setting up the terminal and coordinating training.
6. PI/Project Director must demonstrate PCI DSS compliance by completing the appropriate PCI DSS SAQ and sign the attestation to validation prior to acceptance of any payment transactions.

Merchant Account Set-Up Requests – Internet Transactions

On occasion, there may be a valid business case for a project to accept credit card payments via the internet. At no time should projects process, store or transmit credit card data on any network. Instead, transactions must be completed on approved, secure, fully hosted third party payment processing service. **The cardholder data must be entered directly in the Service Provider's site.** Customers must be re-directed from a project website using a link to an approved third party service provider site.

Projects shall not enter into an outsourcing agreement with a third-party provider, including software applications for credit card processing, until the business case is approved. Third party processors must be PCI DSS compliant, approved by Visa and MasterCard to accept credit card transaction securely over the internet, pre-approved by Elavon and approved by SDSURF. All third parties with access to cardholder data shall be required to acknowledge responsibility for the security of cardholder data in their possession and be contractually required to adhere to PCI DSS compliance, including an annual validation of compliance through methods authorized by a PCI certified Quality Security Assessor.

If an internet application will be utilized, approval from the appropriate network administrator will also be required.

1. Complete a Merchant Account Request Form.
2. Submit completed form to the Merchant Services Coordinator, SDSURF Finance & Accounting, MC 1947.
3. The request form will be reviewed and the appropriate services determined.
4. Once approved, the information will be forwarded to Elavon, who will process the request and issue a merchant id number.
5. Elavon will mail a new merchant welcome kit and contact the merchant directly to walk designated project personnel through the process of setting up the connection to the payment gateway service and coordinating training.

6. PI/Project Director must demonstrate PCI DSS compliance by completing the appropriate PCI DSS SAQ, obtain a certificate of validation of a clean network scan, and sign the attestation to validation prior to acceptance of any payment transactions.

One-Time/Infrequent Events

On occasion, projects may be interested in accepting payments for one-time or infrequent events, such as conference registration or fundraising events. In these cases, it is not practical to set the project up with a merchant account. However, SDSURF maintains a merchant account that can be utilized by authorized projects on a temporary, as-needed basis. An online credit card processing link or wireless terminal will be temporarily provided to the project for payment processing.

1. Complete a Online Credit Card Processing Request Form.
2. Submit completed form to the Merchant Services Coordinator, SDSURF Finance & Accounting, MC 1947.
3. The request form will be reviewed and the appropriate services determined.
4. Check out wireless POS terminal or receive online credit card processing link
5. Check in wireless POS terminal, batch receipts and cash receipts
6. The appropriate PCI DSS SAQ is completed by the Merchant Services Coordinator.

Mail Order, Telephone Order Transactions

Credit card transactions must include the following: cardholder name, card number and expiration date, description of merchandise or services provided, transaction date, and authorized signature.

The project assumes all risks associated with accepting mail order, telephone order, and delayed delivery, including, but not limited to, fraudulent sales transactions. As stated in the PCI standards, credit card numbers, expiration dates and any other cardholder information must be housed in a secure and limited access environment. Do not store credit card information in e-mail, on local desktop/laptop computers or shared network devices. Credit card numbers should be destroyed after the completion of services provided.

Processing Payments

- All face-to-face transactions should have the payment card present and obtain a signature. Compare signatures and check for ID where possible and feasible.
- Always verify that the card is valid and signed. Verify the expiration date.
- Charge cards shall be accepted for no more than the amount of purchase.
- The customer receives the copy of the sales draft that has only four (4) digits on the credit card number. The department retains the other copy and must securely store these drafts.
- Credit card numbers should not be sent via e-mail or fax.
- Credit card numbers should not be entered on a computer or electronic device other than the POS terminal.

- If transmitting transactions using a terminal, settle the transactions daily. This settlement process is called ‘batching out’.
- Merchants should not, under any circumstances, pay any card refund or adjustment to a cardholder in cash.
- 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.
- Merchants are prohibited from engaging in mail/telephone order transactions unless it was indicated on the original application/sales agreement that you accepted or planned to accept such transactions or you have received subsequent written approval to do so from Finance & Accounting.

Cash Receipts

Settlement for merchant card services is done through First Republic Bank. Projects should close out ‘batches’ of charges daily and prepare a SDSURF Cash Receipt form for the amount of the batch. Cash receipts should be delivered in a timely manner to the cashier’s office for processing. *All cash receipts for batches processed in a month are due to the cashier’s office no later than the second business day of the following month.*

Note: No cardholder data should be attached to the cash receipts. Batch receipts should be attached to the cash receipt. Batch receipts that include card numbers should have all but the last four digits masked.

Chargebacks and Disputes

Merchants shall review and resolve any disputes between the customer and their credit card merchant account in a timely manner.

Reconciliation Procedures

All merchant services are settled through First Republic Bank and deposited in an account designated for merchant card services (Bank 15/Bank 16). Detailed statements are available on-line via Elavon’s “Merchant Connect” tool for most merchant accounts. Summary (batch settlement) are available on-line at month end via First Republic Bank. In cases where the project has contracted with a third-party vendor other than Elavon (e.g. KPBS - iMIS–, etc.), a lump sum ACH payment is received by First Republic Bank, detailed statements are not available.

The merchant account bank statement is reconciled with cash receipts on a monthly basis.

DEFINITIONS:

Cardholder – The customer to whom a credit card or debit card has been issued or the individual authorized to use the card.

Cardholder data – All personally identifiable data about the cardholder gathered as a direct result of a credit or debit card transaction (e.g. account number, expiration date, etc.). Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration data, name, address, social security number, Card Validation Code, or CID – Card Identification Number.

Card-validation code – The three-digit value printed on the signature panel of a payment card used to verify card-not-present transactions. On a MasterCard payment card this is called CVC2. On a Visa payment card this is called CVV2.

Credit or Debit Card Receipt Transactions – Any collection of cardholder data to be used in a financial transaction whether by facsimile, paper, card presentation or electronic means.

Credit Card Processor – A third party vendor who processes credit card transactions, routes payments to a merchant's account, charges discount and adjustment fees and generates statements.

Database – A structured electronic format for organizing and maintaining information that can be easily retrieved. Simple examples of databases are tables or spreadsheets.

Electronic Commerce (eCommerce) – is the termed used to define business transactions conducted using an electronic medium.

Encryption – The process of converting information into a form unintelligible to anyone except the holders of a specific cryptographic key. Use of encryption protects information from unauthorized disclosure between the encryption process and the decryption process.

Firewall – Hardware and/or software that protect the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows it workers access to the wider Internet must have a firewall to prevent outsiders from accessing its own private data resources.

Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe used for authorization during a card present transaction. Magnetic stripe or 'magstripe' data contains the cardholder name, account number, encrypted PIN, and other discretionary data.

Merchant – Any Project/Organization that participates in card processing activities.

Merchant Account – An account established by contractual agreement between a merchant/business and a bank or payment gateway.

Merchant Card Coordinator (Deanna Vaughn) – Position that serves as the interface between the merchant bank and merchants. Provides support, training, and general services to merchants in all areas relating to payment card processing (e.g. reconciliations, disputes, compliance).

Network – A network is defined as two or more computers connected to each other so they can share resources.

Online Credit Card Acceptance – Credit card payments are submitted via the web using a third party vendor's software and passed onto the credit card processor for real-time authorization.

The third party vendor security accepts and stores credit card information in compliance with the credit card company's security requirements.

Payment Card – credit cards, debit cards, ATM cards, and any other card or device, other than cash or checks, issued by a bank or credit union, which is normally presented by a person for the purpose of making a payment.

Payment Application – Software vendors, who develop applications that store, process or transmit cardholder data as part of authorization or settlement.

Payment Gateway – A service provided by a billing processor, which allows credit card information to be collected and passed over the internet. A payment gateway can be thought of as a digital equivalent to a credit card processing terminal. Some payment gateways establish or resell merchant accounts. --- A service provided by a billing processor, which allows credit card information to be collected and passed over the internet. A payment gateway can be thought of as a digital equivalent to a credit card processing terminal. Some payment gateways establish or resell merchant accounts. A category of agent or service provider that stores, processes, and/or transmits cardholder data as part of a payment transaction.

Primary Account Number (PAN) – The payment card number (credit or debit) that identifies the issuer and the particular cardholder account.

PCI – Purchasing Card Industry Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

PCI DSS – The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

PCI DSS Standards – The Payment Card Industry (PCI) Data Security Standard was created by major credit card companies to safeguard customer information. Visa, MasterCard, American Express and other credit card associations mandate that merchants and service providers meet certain minimum standards of security when they store, process and transmit cardholder data.

Privileged Access – Access to more than one card number at a time, as opposed to access to a single card number for purposes of completing a transaction (Thus, the term describes positions such as database administrators of systems that house cardholder data, but not cashiers handling one card at a time.)

Service Providers – The third parties SDSU or SDSURF has contracted with who are involved in the processing of credit card transactions. This includes the credit card processor and online credit card acceptor. Organizations that process, store, or transmit cardholder data on behalf of members, merchants, or other service providers.

System Administrator / Data Custodian – An individual who performs network or system administration duties and/or technical support of network or systems that are accessed by other people, systems, or services.

Wireless Technology – Includes any technology used to transmit data without a physical connection.

Appendix A – Sample Contract Language

SDSURF Clause

Contractor is currently certified to be in compliance with the PCI Security Standards Council's Payment Card Industry Data Security Standards, including the current published version by a qualified security assessor (QSA) and approved scanning vendor (ASV), as applicable. Any changes in Contractor's certification require prompt written notification to the client. Contractor agrees to continue to meet all PCI DSS requirements and to validate compliance annually according to the credit card industry rules, which include but are not limited to the Payment Card Industry Data Security Standards. Contractor will also provide written evidence of this compliance to the SDSU Research Foundation annually. If applicable, Contractor agrees that its electronic check processing functionality will comply with the appropriate NACHA- the Electronic Payment Association provisions. Applications purchased from a third party that will be used by a Merchant to store process or transmit sensitive cardholder data must be Payment Application Best Practices (PABP) certified. This certification ensures that the application is compatible with Payment Card Industry Data Security Standard requirements. Information about PABP validation is available from Visa.