Title of the Policy: PCI DSS Compliance Policy

Functional Area: Finance and IT Services

Applies To: See Scope Section Below

Policy Reference(s): PCI Security Standards Council

Number: Version 1.0

Date Issued: 2 February 2016

Page(s): 20

Responsible Person

The Vice President for Business and Finance is responsible for implementing and revising this policy.

Purpose / Rationale

This document and additional supporting documents represent Armstrong State University’s policy to prevent loss or disclosure of customer information including credit card numbers. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the unit and the university.

Scope

The Armstrong State University Payment Card Procedures apply to all faculty, staff, students, organizations, third-party vendors, individuals, systems and networks involved with payment card handling. This includes transmission, storage and/or processing of payment card data, in any form (electronic or paper), on behalf of Armstrong State University.
## Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payment Card Industry Data Security Standards</strong></td>
<td>The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Payment card Brands: Visa, MasterCard, American Express, Discover, JCB</td>
</tr>
<tr>
<td><strong>Cardholder</strong></td>
<td>Someone who owns and benefits from the use of a membership card, particularly a payment card.</td>
</tr>
<tr>
<td><strong>Card Holder Data (CHD)</strong></td>
<td>Those elements of payment card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Card Identification Number (CID).</td>
</tr>
<tr>
<td><strong>Primary Account Number (PAN)</strong></td>
<td>Number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.</td>
</tr>
<tr>
<td><strong>Payment Card</strong></td>
<td>Refers to both credit, debit cards, and university purchase or p-cards.</td>
</tr>
<tr>
<td><strong>Merchant</strong></td>
<td>Refers to an Armstrong department or operating area that has applied for and been approved to accept credit/debit card payments by the Controller. A merchant is assigned a specific merchant account (MID), which is used to process all credit/debit card transactions via an Armstrong-approved payment card processor.</td>
</tr>
<tr>
<td><strong>Payment Card Processor</strong></td>
<td>The entity engaged by a merchant to handle payment card transactions on its behalf and can also be referred to as a “payment gateway”. Payment processors are not considered acquirers.</td>
</tr>
<tr>
<td><strong>Point of Sale (POS)</strong></td>
<td>This is the location where payment card information is taken to complete a purchase by the cardholder.</td>
</tr>
<tr>
<td><strong>Service Provider</strong></td>
<td>Any company that stores, processes, or transmits cardholder data on behalf of another entity is defined to be a Service Provider by the Payment Card Industry (PCI) guidelines.</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>In-scope cards include any debit, credit, and pre-paid cards branded with one of the five card association/brand logos that participate in the PCI SSC – American Express, Discover, JCB, MasterCard, and Visa International. PCI Scope includes Payment Gateways that connect a merchant to the bank or processor that is acting as the front-end</td>
</tr>
</tbody>
</table>
connection to the Card Brands. They are called gateways because they take many inputs from a variety of different applications and route those inputs to the appropriate bank or processor. Gateways communicate with the bank or processor using dial-up connections, Web-based connections or privately held leased lines.

<table>
<thead>
<tr>
<th><strong>SAQ</strong></th>
<th>The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI DSS self-assessment.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acquiring Bank</strong></td>
<td>Typically a financial institution that processes payment card transactions for merchants. It is defined by a payment brand as an acquirer.</td>
</tr>
<tr>
<td><strong>Magnetic Stripe (i.e., track) data</strong></td>
<td>Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.</td>
</tr>
<tr>
<td><strong>CAV2, CVC2, CID, or CVV2 data</strong></td>
<td>The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.</td>
</tr>
<tr>
<td><strong>Merchant Department</strong></td>
<td>Any department or unit (can be a group of departments or a subset of a department) which has been approved by Armstrong State University to accept payment cards and has been assigned a Merchant identification number.</td>
</tr>
<tr>
<td><strong>Merchant Department Responsible Person (MDRP)</strong></td>
<td>An individual within the department who has primary authority and responsibility within that department for payment card transactions.</td>
</tr>
</tbody>
</table>

**Policy**

**PCI DSS**

The PCI DSS (Payment Card Industry Data Security Standard) is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org)

In order to accept credit card payments, Armstrong State University must prove and maintain compliance with the Payment Card Industry Data Security Standards. The Armstrong State University PCI DSS Policy and additional supporting documents provide the requirements for the processing, transmission, storage and disposal of cardholder data of payment card transactions in order to reduce the institutional risk associated with the administration of credit card payments by university departments to ensure proper internal control and compliance with the Payment Card Industry Data Security Standard (PCI-DSS).
PCI DSS GOALS

Build and Maintain a Secure Network

1. Install and maintain a firewall and router configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access while implementing secure authentication controls through such methods as password restrictions and guidelines, passphrase or two-factor authentication.
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for employees and contractors.

Responsibilities

PCI Steering Committee (PSC)

This cross functional committee is the principal decision making body at Armstrong State University in matters regarding PCI compliance. Members of the committee may vary from time to time but the following individuals will always be members: Vice President for Business and Finance, AVP for Finance, Foundation Controller, CIO, Information Security Officer (ISO), Director of Budget & Auxiliary Services, and the Director of Internal Audit.
The PSC is responsible for the following:

1. Creating effective lines of accountability, responsibility and authority for compliance with the PCI DSS and Payment Application Data Security Standards (PA-DSS)

2. Approving policies, procedures, and guidelines related to PCI DSS compliance;

3. Providing input in the Emergency Management Plan in the event of a data breach;

4. Overseeing the building and maintaining of secure networks, payment applications, systems and related infrastructure;

5. Approving new merchants who wish to begin accepting credit card payments to be PCI compliant before accepting payment card transactions; The PSC will follow up to review and approve all applications for new merchant accounts and any variances to normal merchant operations for existing merchants.

6. Facilitating and scheduling ongoing network scanning and penetration testing for applicable merchants;

7. Implementing new mandates issued by the PCI Security Standards Council and conforming to the evolving PCI DSS;

8. Assisting merchants in reducing their PCI scope to minimize the chance of a data breach

9. Assisting the AVP for Finance in bringing non-responsive, non-compliant merchant departments into compliance prior to their payment card privilege being terminated;

10. Providing annual security awareness & training programs

The PSC may designate working groups or subcommittees to accomplish these responsibilities, but the PSC retains ultimate responsibility for PCI compliance.

Chief Information Officer

Information Technology Services (ITS) is responsible for the following:

1. Maintaining and disseminating security policies and procedures that address PCI DSS requirements

2. Testing Armstrong’s infrastructure and network environment

3. Assisting the PCI Steering Committee in completing the technical sections of the annual PCI DSS self-assessment questionnaire (SAQ)

4. Configuring and managing applications and infrastructure that store, process or transmit cardholder data in compliance with PCI DSS and Armstrong security requirements

5. Establishing appropriate limits for access to IT resources and cardholder data.
AVP for Finance
The AVP for Finance is responsible for the following:

1. Establishing agreements with acquiring banks
2. Overseeing the initial setup and ongoing administration of all university merchant accounts.
3. Previewing merchant applications before submission to the PSC.
4. Reviewing third-party credit card processing vendors and service providers for compliance.

Departmental Merchants
Departmental Merchants are responsible for the following:

1. Ensuring that all business process documents for accepting, processing, retaining, and disposing of cardholder data are updated and comply with the PCI DSS Policy and all other applicable policies and standards
2. Performing an annual PCI DSS self-assessment

Departmental Employees
Departmental employees who are involved in the storing, processing, transmitting, or have access to cardholder data are responsible for:

1. Completing PCI DSS training upon hire and at least annually. All employees will acknowledge reading and understanding these security policies and procedures, and will comply with these policies.

Procedures

In the course of doing business at Armstrong State University, or its affiliated organizations, it may be necessary for a department or other unit to accept payment cards for payment. Armstrong State University requires all departments that accept payment card payments to do so only in compliance with payment card industry standards and in accordance with the following procedures.

Card Acceptance and Handling

1. All credit card processing is subject to review by the PSC. This includes credit card payments received via: web forms, walk-in, phone calls, faxes, or mail; and off-site events.

2. POS (point of sale) or card swipe terminals must be approved by the PSC and used only with dial-out connections or locked-down internet terminals.

3. Employees and students handling cardholder information are encouraged to go through a background check and must acknowledge understanding of these Armstrong Credit Card Processing Guidelines. Generally, students should not have access to cardholder information. Anyone handling cardholder information will be required to attend such training on an annual basis.
4. The opening of a new merchant account for the purpose of accepting and processing payment cards is done on a case by case basis. Any fees associated with the acceptance of the payment card processing in that unit will be charged back to the unit.

4.1. Interested departments or units should contact the Assistant Vice President for Finance to begin the process of accepting payment cards. Steps include:

4.1.1. Completion of an “Application to become a Merchant Department” (Attachment A)

4.1.2. Completion of training

4.1.3. Read and sign-off attesting to their understanding of this policy and its requirements. The attestation statement is included in the Application (see Attachment A).

4.1.4. Applications are submitted to the Assistant Vice President for Finance for review and then forwarded to the PSC for final approval / rejection.

5. Any department accepting payment cards on behalf of the institution or related foundation must designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions. This individual is referred to as the Merchant Department Responsible Person or MDRP. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the MDRP is unavailable.

6. Merchant Account Fees for University Departments: The budget/department which owns the merchant and receives the benefit of the revenue is responsible for all costs associated with payment card processing. These costs include, but are not limited to, merchant account setup and administrative fees, equipment purchases, recurring monthly costs, and fees based on a percentage of every transaction from each credit card brand.

7. Card Acceptance
   7.1. Obtain the signature of the cardholder on the receipt

   7.2. Verify signature of cardholder at the time of the transaction for card-present transactions.

   7.3. Verify that the payment card’s expiration date is valid.

   7.4. Verify that only the last four digits of the payment card number are printed on the receipt and provide a duplicate copy to the cardholder.

   7.5. If accepting cardholder data via fax, locate the fax machine in a secured, non-public area with limited access.
7.6. Payment card charges should not exceed the transaction amount of purchase.

7.7. Refunds must be made to the payment card that was used during the transaction. No transactions should be refunded in cash or to a different payment card.

7.8. Do not accept cardholder data utilized via end-user messaging technologies (e.g., e-mail, voicemail, instant messaging, and text messaging).

8. Annual PCI DSS Self-Assessment: The Controller will contact each merchant to schedule their annual self-assessment. Each merchant must complete an annual self-assessment questionnaire to attest compliance with this policy, PCI DSS, and other applicable standards and policies. Merchants found not in compliance will work with the Controller to implement the appropriate remediation activities.

9. Specific details regarding processing and reconciliation will depend upon the method of payment card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and will be also available by contacting the Controller.

10. All service providers and third party vendors that provide payment card services must be PCI-DSS compliant. Departments who contract with third-party service providers must maintain a list that documents their service providers and:

10.1. Ensure contracts include language that states that the service provider or third party vendor is PCI compliant and will protect all cardholder date (see Attachment B for sample language.)

10.1.2. Annually audit the PCI compliance status of all service providers and third-party vendors. Frequent lapses in PCI compliance will result in termination of the relationship.

Payment Card Data Security

Procedures must be documented by authorized departments and be available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis:

Processing and Collection:

1. Collected cardholder data must be restricted only to those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access and review the list monthly.

2. All equipment used to collect data must be secured against unauthorized use or tampering in accordance with the PCI Data Security Standard. All workstations used for entering cardholder information into online web forms must be locked-down.

3. Email should not be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information. If payment card data is received in an email:
The email should be replied to immediately with the payment card number deleted stating that Armstrong State University does not accept payment card data via email as it is not a secure method of transmitting cardholder data. The reply email should not include the cardholder information.

The email should be deleted from the inbox and from the trash.

Storage and Destruction:

The goal of the PCI Data Security Standard (PCI DSS) is to protect cardholder data and sensitive authentication data wherever it is processed, stored or transmitted. The security controls and processes required by PCI DSS are vital for protecting all payment card account data, including the PAN – the primary account number printed on the front of a payment card. Merchants, service providers, and other entities involved with payment card processing must never store sensitive authentication data after authorization. This includes the 3- or 4-digit security code printed on the front or back of a card, the data stored on a card’s magnetic stripe or chip (also called “Full Track Data”) and personal identification numbers (PINs) entered by the cardholder.

1. Cardholder data, whether collected on paper or electronically, must be protected against unauthorized access. Any media, including paper copies that contain cardholder information, must be treated as confidential.

2. Physical security controls must be in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents or electronic files containing cardholder data. Any paper copies of cardholder information must be securely stored in a locked location when not in use.

3. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, tablets, compact disks, floppy disks, USB flash drives, personal digital assistants, and portable external hard drives.

4. Cardholder data should not be retained any longer than a documented business need; after which, it must be deleted or destroyed immediately following the required retention period. The maximum period of time the data may be retained is for a maximum of three credit card billing cycles. A quarterly schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the record retention requirements.

5. Purchasing Card data shall be protected in a similar manner and institute the above components, particularly in regards to storage and disposal of cardholder data.

6. Hand deliver manual credit card payment slips or Direct Deposit Reports that include credit card processing data to the Bursar’s Office on a daily basis using a secure envelope and a procedure for verifying delivery.
7. Do not publicly display cardholder information or leave it unattended; do not disclose cardholder information to others.

8. When paper copies of cardholder information are no longer necessary, they must be shredded using a PCI-compliant crosscut shredder.

Training

The PSC will provide and the AVP for Finance will implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. The program will include web-based and in-person formal training, as well as notifications to employees on security topics, such as malware outbreaks and phishing scams. This training satisfies PCI compliance standard 12.6.1.

The PSC will provide and the AVP for Finance will implement training for personnel to be aware of attempted tampering or replacement of devices. This will be required for any departments that utilize equipment that can directly interact with a card, even if not utilized for that purpose. Common examples of points of interaction (POI) are stand-alone POS terminals such as Verifone or Ingenico devices, USB-connected “wedge” readers, or readers incorporated into POS registers, such as readers embedded into a Micros terminal. This training satisfies PCI compliance standard 9.9.

The PSC will provide training and the Information Security Officer will implement the appropriate training of staff with security breach response responsibilities. This training satisfies PCI compliance standard 12.10.4.

Data Breach Procedures

1. Anyone who learns of an actual or potential cardholder data security breach, including the suspicion that payment card data has been exposed, lost, stolen, or misused, must immediately inform the ITS Help Desk and the University Controller.

2. Indications that such an investigation may be necessary include, but are not limited to, the following:

   2.1. A computer or device involved in credit card processing is compromised. You may observe a virus or other malware installed on the system or that unauthorized configuration changes have been made that cannot be adequately explained.

   2.2. Vulnerability is discovered that could be used to gain unauthorized access to cardholder data.

   2.3. An external report is received that indicates that Armstrong may be a source of fraudulent transactions, or that cardholder data from Armstrong has been accessed without authorization.

   2.4. Paper, tapes, USB-keys, laptops, or other media containing cardholder data has been lost or cannot be accounted for.

   2.5. Cardholder data has been discussed in public or overheard without authorization.
2.6. Any of the above occurs with a service provider or other third party involved in payment card processing for Armstrong.

3. In the event a cardholder data breach involving non-electronic resources (for example, paper documents) is suspected, the Controller must be notified immediately.

4. If you suspect credit card fraud, please notify the Controller immediately

**Enforcement and Ongoing Compliance**

Periodic reviews of safeguarding and storing of payment card information are conducted by the University Controller, and payment card handling procedures are subject to audit. In addition, the Armstrong IT Services periodically conducts assessments of security controls put in place to safeguard technology implementations, including but not limited to periodic network based vulnerability scans. Armstrong schools/units with Merchant Account Numbers that do not comply with this policy and approved protection, storage, and processing procedures may lose the privilege to serve as a payment card merchant and to accept payment card payments.

Individuals in violation of this policy are subject to the full range of sanctions.

**Hardware and Network Security**

The following safeguards will be implemented:

1. router and switch configurations
2. vulnerability management
3. log management
4. penetration testing
5. access management

Vendor-provided security patches will be installed on a monthly basis for non-critical patches. Patches that are deemed critical are applied once released and tested. All critical systems must have the most recent released software patches to prevent exploitation. An outside vendor validates the security standings of the PCI network by performing annual penetration tests. Internal system scans are performed on a monthly basis to ensure patch levels are met.

1. System resources are tracked and monitored allowing the ability to track user activities that are critical for effective forensics and vulnerability management.

2. Log monitoring is used to help with the tracking and analysis of actions on the PCI network and resources.

3. Anti-virus software is a requirement on all systems as this serves to protect systems from current and evolving malicious software threats.

4. Each user with access to PCI resources will be assigned an account with a unique identification (ID) that allows IT the ability to track and monitor the actions that are taken on all critical data and systems.
5. Asset inventory and tracking is performed to safeguard the University from the possibility of theft for information, equipment and license agreements. Knowing your resources and requirements are a must to keep your environment safe and compliant.

In order to support standardization, all changes for resources on the PCI network must go through IT Services Change Management process. This process includes a formal request and approval process prior to any changes being made. This process enables documentation of the resources to be kept current while coordinating the efforts of people to accomplish their goals and objectives effectively.

**Third Party Service Providers**

Third-party vendors and service providers contracted by Armstrong must process payment cards and handle cardholder data according to the PCI DSS. Armstrong reserves the right at any time to request proof of PCI DSS compliance via an attestation of compliance verifying that the vendor/service provider uses secure standard financial industry practices in its financial transactions. Alternately, the vendor is considered compliant if they appear on one of the global registries listed below:

- VISA Global Registry of Service Providers
- MasterCard Compliant Service Provider List

**POS Device Security**

PCI compliance requires that all merchants must have controls in place to protect against direct physical tampering and substitution of their card-reading devices used in card-present transactions at the point of sale. This requirement applies to any card swipe (or dip) POS device or terminal used in face-to-face transactions (including any unattended payment terminals accepting transactions where the customer’s card is present). In summary, the protection requirements are:

1. Maintain an up-to-date inventory of your terminals/devices

2. Periodically inspect terminals/devices to look for tampering or substitution

3. Train personnel to be aware of suspicious behavior and to report tampering or substitution of devices/terminals

4. Check for simple abnormalities. A missing seal or screw, or extra wiring or holes, for instance, could be the first step to uncovering fraud. You should also look out for added labels, decals or other materials that may be masking damage inflicted by tampering.

5. Routinely inspect POS terminals and PIN-entry devices (PEDs) and secure terminals to counters to prevent removal.

6. Secure your POS devices.
7. All new employees should review the Skimming Prevention document before engaging in merchant activities and then review annually.

Risk Assessment

Annually, the Internal Auditor will facilitate a formal Risk assessment process in which current threats and vulnerabilities to Armstrong’s networking and processing environment are analyzed. The internal auditor will prepare a report including recommendations and deliver to the PSC who will review the report and develop a corrective action plan.
APPENDIX A
APPLICATION TO BECOME A MERCHANT DEPARTMENT

1. DEPARTMENT INFORMATION:

DEPARTMENT NAME: ____________________________________________

MERCHANT (LOCATION) NAME: ____________________________________________

Note: The merchant (location) name will appear on your customer’s monthly statements and on the bank statements sent to the Controller’s Office

INTERNET ADDRESS: ____________________________________________

Note: The merchant (location) name will appear on your customer’s monthly statements and on the bank statements sent to the Controller’s Office

MERCHANT (LOCATION) ADDRESS: ____________________________________________

Note: Merchant address must include Building & Room number. Statements will be mailed to this address.

2. PRIMARY CONTACT INFORMATION:

CONTACT NAME: ___________________________ MAIN TELEPHONE #: ___________________________

CONTACT TITLE: ___________________________ ALT. TELEPHONE #: ___________________________

EMAIL ADDRESS: ___________________________ FAX NUMBER: ___________________________

Note: The primary contact will be responsible for the overall process of accepting payment cards at this location and must be a full time employee. (A work-study student is not allowed to serve as a primary contact).

3. MERCHANT INFORMATION:

GIVE A BRIEF DESCRIPTION OF YOUR PAYMENT CARD BUSINESS: (What is the main purpose of this merchant account? For example, registration fees, tuition for non-credit courses, tickets for events)
DATE SUBMITTED: ____________________ DESIRED “LIVE” DATE: ____________________

TRANSACTION TYPE TO BE ACCEPTED (Mark with an X): Note: Debit cards will be processed the same as credit cards.

( ) VISA ( ) DEBIT ( ) AMERICAN EXPRESS
( ) MASTERCARD ( ) DISCOVER

ESTIMATED ANNUAL CREDIT CARD VOLUME:
Total Annual Dollar Amount: $ ____________________

Average Amount per Transaction: $ ____________________

Annual Number of transactions:

________________________________________

PROCESSING TYPES (Check the types of system currently being used or that will be used):
( ) POS Terminals ( ) Internet (Online) ( ) Other

If Other, describe in detail:

________________________________________

Current Third Party Vendor, if applicable:

________________________________________

CHARGEBACK INFORMATION:
Mail “Chargebacks” to (Provide name, title, and address including building and room #)

CONTACT NAME: __________________________ ADDRESS:

CONTACT TITLE: __________________________

Note: Chargebacks are created when a customer disputes a charge. If action is not taken by the merchant within the time frame indicated on the letter, Armstrong State University will be charged by the payment card company. A journal entry must be made by the merchant to record such chargeback. The merchant should contact the Controller’s Office with information to complete the journal entry.

IF PROCESSING USING A POINT OF SALE (POS) ELECTRONIC TERMINAL, PLEASE PROVIDE:

<table>
<thead>
<tr>
<th>MODEL</th>
<th>FIRMWARE/SOFTWARE VER.</th>
<th>SERIAL NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IF PROCESSING OVER THE INTERNET, PLEASE PROVIDE:

CONTACT
NAME: __________________________ TELEPHONE #: __________________________
(Technical)

CONTACT
TITLE: __________________________ EMAIL ADDRESS: __________________________

FOR PROCESSING JOURNALS, PLEASE PROVIDE:

CONTACT
NAME: __________________________ TELEPHONE #: __________________________

CONTACT
TITLE: __________________________ EMAIL ADDRESS: __________________________

FOR PROCESSING CHARGEBACKS, PLEASE PROVIDE:

CONTACT
NAME: __________________________ TELEPHONE #: __________________________

CONTACT
TITLE: __________________________ EMAIL ADDRESS: __________________________

DEPARTMENT ACCEPTS PAYMENT CARDS: (Check all that apply)

(    ) IN PERSON

(    ) BY PHONE

(    ) BY MAIL

(    ) BY FAX

(    ) ON-LINE PAYMENT VIA UNIVERSITY’S APPROVED INTERNET PROCESSOR (name of provider) __________________________

(    ) ON LINE PAYMENT VIA OTHER, NAME: __________________________
CHECKLIST / ATTESTATION

1. I have read, understand, and agree to abide by Armstrong’s PCI DSS Compliance Policy
2. I will utilize cardholder data for Armstrong business purposes only.
3. I will not use or distribute cardholder data for personal purposes. I understand that such actions are illegal and grounds for prosecution.
4. I understand that in cases where I suspect a breach of security, including the suspicion that cardholder data has been exposed, lost, stolen, or misused, I must immediately contact the Controller’s Office.
5. If I am the Merchant Department responsible person, I understand that I must maintain documented and effective business processes for accepting, processing, retaining, and disposing of cardholder data.
6. I understand that failure to comply with this policy and/or applicable policies, standards, and procedures carries severe consequences, which may include loss of the ability to process payment card transactions and disciplinary action, which can include termination of employment.
7. I and the appropriate members of my staff have completed PCI awareness training.
8. The members of my staff who will be processing transactions, including myself if applicable, have received training on how to operate an electronic terminal.
9. I will ensure that documents that contain sensitive payment card information are shredded in a cross-cut shredder immediately after the transaction is processed.
10. I will ensure that payment card numbers are truncated on the receipt.
11. I will ensure that the electronic terminal(s) will be kept in a secured and restricted area, away from public access.
12. I will limit the number of employees who process payment cards to appropriate employees based on their job duties.
13. I will keep the Office of the Controller aware of any changes in my payment card program.
14. I will ensure that access to payment card processing is revoked immediately upon the termination of any of my employees.
15. I will ensure that cardholder data and other sensitive information is stored according to the guidelines set forth in this policy.
16. I will ensure that the default security settings, accounts, and passwords on production systems are changed before taking the systems into production.
17. I will ensure that transmission of cardholder data and other sensitive information across public networks is encrypted using SSL or other industry acceptable methods.
18. I will ensure that an anti-virus scanner is installed on all servers and all workstations and that the virus scanner is regularly updated.
19. I attest that I have read the checklist for merchants and have completed or have in place all necessary requirements for merchant card processing.
CHECKLIST / ATTESTATION

Continued

Authorized Signature: ___________________________ Date: __________________

Printed Name: ________________________________ Telephone #: ______________

Title: ________________________________________ Armstrong ID: ____________
INFORMATION FOR THIRD PARTY PROCESSORS OR GATEWAYS:

If you are not using a Third Party Processor or Gateway, please skip this section.

1. Do you have a written agreement with an acknowledgment that indicates that the service provider (vendor) is responsible for the security of cardholder data?

   YES ( )  NO ( )  If NO, please explain ________________________________

2. Has the written agreement been reviewed and approved by our Legal Department?

   YES ( )  NO ( )  If NO, please explain ________________________________

3. Has the written agreement been reviewed and approved by Information Technology?

   YES ( )  NO ( )  If NO, please explain ________________________________

4. Has the service provider (vendor) supplied you with a certificate of Payment Card Industry Data Security Standards (PCI DSS) compliance?

   YES ( )  NO ( )  If NO, please explain ________________________________

5. Do you request a certificate of PCI DSS compliance annually from the service provider (vendor)?

   YES ( )  NO ( )  If NO, please explain ________________________________

6. Are development, testing, and production systems updated with the latest security-related patches released by the vendor?

   YES ( )  NO ( )  If NO, please explain ________________________________

7. Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?

   YES ( )  NO ( )  If NO, please explain ________________________________

8. Are unused services/applications on servers completely disabled/removed from all production environments, for security, increased system performance, and to improve system stability (for carrying out database, FTP, email, or web-hosting related task?  

   YES ( )  NO ( )  If NO, please explain ________________________________
APPENDIX B

SUGGESTED CONTRACT LANGUAGE FOR SERVICE PROVIDERS

PCI DSS Requirement 12.8 requires merchants to maintain and implement policies and procedures to manage Service Providers if cardholder data is shared. Requirement 12.8.2 states further “maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.”

The language below could be used as an Addendum to present in contracts with Service Providers.

(Company) is responsible for the security of credit card information in its possession. (Company) will inform Armstrong State University within twenty-four hours if it has knowledge of, or can reasonably expect that, a security breach has occurred. (Company) takes responsibility for the payment of fines, penalties, lawsuits and other costs incurred by Armstrong State that result from a breach that can be traced to the action or inaction of (Company) and will assume 100% of those costs assuming no contributory negligence on the part of Armstrong State University, merchant acquirer, merchant bank, or other negligent third party.

(Company) Obligations: The (Company) agrees to: (1) comply with Payment Card Industry (PCI) Data Security Standard (PCI DSS) and undergo Level 1 PCI audits as necessary; (2) maintain PCI DSS Level 1 compliance through the duration of the Agreement; (3) keep data confidential and not copy, publish, sell, exchange, disclose or provide to others or use any information, documents or data, provided or disclosed to the (Company) or any account information related to credit cards or cardholders for any purpose other than performing the (Company's) obligations under the Agreement; (4) maintain the security and confidentiality of card transactions processed through <Service Provider Service> (while the information is stored within <Service Provider Service>); and (5) ensure that all <Service Provider Service> interfaces are compatible with the requirements of the processing systems and networks established and used by a Merchant Acquirer.

Regarding (3) above, (Company) agrees to provide to Armstrong State University a copy of the Confirmation of Report Accuracy (CORA) and the Certificate of Validation (COV) as submitted annually by a Qualified Security Assessor (QSA) to Visa and MasterCard, respectfully. Further, (Company) agrees to provide to Armstrong State University a copy of proof of successfully passing the quarterly external scan as submitted by an Approved Scanning Vendor (ASV).