



Proposed Policy Number and Title: 457 PCI DSS Compliance		
Existing Policy Number and Title: Not applicable		
<b>Approval Process*</b>		
<input checked="" type="checkbox"/> Regular	<input type="checkbox"/> Temporary Emergency	<input type="checkbox"/> Expedited
<input checked="" type="checkbox"/> New	<input type="checkbox"/> New	<input type="checkbox"/> New
<input type="checkbox"/> Revision	<input type="checkbox"/> Revision	<input type="checkbox"/> Revision
<input type="checkbox"/> Deletion	<input type="checkbox"/> Suspension	
	Anticipated Expiration Date:	
*See UVU Policy #101 <i>Policy Governing Policies</i> for process details.		

<b>Draft Number and Date:</b> <u>Stage 4, Board of Trustees, February 19, 2015</u>		
<b>President's Council Sponsor:</b> <u>Val Peterson</u>	<b>Ext.</b> _____	
<b>Policy Steward:</b> <u>Kedric Black</u>	<b>Ext.</b> _____	

**POLICY APPROVAL PROCESS DATES**

**Policy Drafting and Revision**  
Entrance Date: 08/28/2014

**University Entities Review**  
Entrance Date: 09/25/2014

**University Community Review**  
Entrance Date: 12/18/2014  
Open Feedback: 12/18/2014  
Close Feedback: 01/14/2015

**Board of Trustees Review**  
Entrance Date: 01/15/2015  
Approval Date: MM/DD/YYYY

**POST APPROVAL PROCESS**  
Verify:

- Policy Number
- Section
- Title
- BOT approval
- Approval date
- Effective date
- Proper format of Policy Manual posting
- TOPS Pipeline and Archives update

**Policy Office personnel who verified and posted this policy to the University Policy Manual**

**Name:** \_\_\_\_\_

**Date posted and verified:** MM/DD/YYYY



<b>POLICY TITLE</b>	PCI DSS Compliance	<b>Policy Number</b>	457
<b>Section</b>	Facilities, Operations, and Information Technology	<b>Approval Date</b>	
<b>Subsection</b>	Information Technology	<b>Effective Date</b>	
<b>Responsible Office</b>	Office of the Vice President of Administration and Finance		

### 1.0 PURPOSE

**1.1** The purpose of this policy is to help ensure that the University 1) serves as an effective steward of personal financial information entrusted to it by its constituents, 2) protects the privacy of its constituents, 3) complies with the PCI DSS, and 4) strives to avoid a security breach aimed at obtaining cardholder information.

**1.2** To minimize inappropriate exposures, losses, and inappropriate use of cardholder data, this policy sets forth a framework to aid the University by complying with PCI DSS and attending to the proper design and control of systems in scope of PCI DSS.

### 2.0 REFERENCES

**2.1** *Payment Card Industry Data Security Standard (PCI DSS)*

**2.2** *UVU 441 Appropriate Use of Computing Facilities*

**2.3** *UVU 443 Ethics in Computer Usage*

**2.4** *UVU 445 Institutional Data Management and Access*

**2.5** *UVU 447 Responsibility for Security of Computing Devices Connected to the UVU Network*

**2.6** *UVU 448 Use of University Technology Equipment*

**2.7** *UVU 451 Retention of Electronic Files*

### 3.0 DEFINITIONS

**3.1 Acquiring bank:** Entity that initiates and maintains relationships with merchants for the acceptance of payment cards. Also referred to as acquirer or acquiring financial institution.



**3.2 Attestation of Compliance (AOC):** The form used for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the *Self-Assessment Questionnaire* or *Report on Compliance*.

**3.3 Cardholder:** Non-consumer or consumer customer to whom a payment card is issued, or any individual authorized to use the payment card.

**3.4 Cardholder data:** At a minimum, cardholder data consists of the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

**3.5 Cardholder data environment:** The people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data, including any connected system components.

**3.6 Computer Incident Response Team (CIRT):** The group, comprised of the Information Security Officer and Senior Security Analysts, that oversees the investigation and remediation of issues that led to a security breach of IT systems.

**3.7 Merchant:** For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI Security Standards Council (American Express, Discover, JCB, MasterCard, or Visa) as payment for goods and/or services.

**3.8 Payment Card Oversight Committee (PCOC):** A group tasked with the oversight of the University's PCI DSS compliance. It is comprised of the Associate Vice President–CIO/Information Technology, Senior Analyst–PCI Security, Officer–Security/IT Services, Controller–Business Services, and the Senior Accountant of Treasury Services.

**3.9 Payment Card Industry Data Security Standard (PCI DSS):** Standards developed by the PCI Security Standards Council (PCI SSC), which provide an actionable framework for developing a robust payment card data security process, including prevention, detection, and appropriate reaction to security incidents.

**3.10 Primary account number (PAN):** Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. Also referred to as account number.

**3.11 Self-Assessment Questionnaire (SAQ):** Tool used by any entity to validate its own compliance with PCI DSS and when filing an AOC. The completed *Self-Assessment Questionnaire* is filed with the entity's acquiring bank.



**3.12 Sensitive authentication data:** Security-related information (including but not limited to card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment-card transactions.

**3.13 Service provider:** Business entity, which is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS, and other services, as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

#### 4.0 POLICY

**4.1** UVU is responsible for its PCI DSS compliance and security breaches that occur on its information systems that handle credit card information; it is not responsible or liable for the PCI DSS compliance of non-university entities that conduct merchant business on university property or for security breaches that occur on the systems of these entities.

**4.2** All merchant entities (both university and non-university entities) wishing to accept, process, transmit, or store payment cards while conducting business on UVU's campus and other university-owned facilities must receive approval from the Payment Card Oversight Committee (PCOC).

**4.3** All merchant entities wishing to accept, process, transmit, or store payment card information while conducting business on UVU's campus and other university-owned facilities must be compliant with the standards set by the PCI SSC. University merchant entities shall provide adequate training for all employees dealing with payment card data on how this data should be handled securely and of the risks associated with payment card data relevant to the scope of their employment duties and shall follow the information security procedures outlined by the PCOC.

**4.4** In order to ensure proper handling and safeguarding of payment card information, merchant entities will work with the PCOC to build and maintain a secure network for payment card information handling. This network shall meet the most current requirements established by the PCI SSC.

**4.5** Each university employee who has access to cardholder information is responsible for protecting that information in accordance with PCI DSS and UVU policy and procedures.

**4.6** All university merchant entities must complete the appropriate *PCI DSS Report on Compliance (ROC)* or *Self-Assessment Questionnaire (SAQ)* and *Attestation of Compliance*



(AOC) and submit both documents to the Finance and Business Services Office annually by the last university working day in June.

**4.7** Non-university merchant entities and service providers operating on any of the University's campuses that accept credit cards must execute a contract addendum that includes an acknowledgement of responsibility for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the University, or to the extent that they could impact the security of the University's cardholder data environment. The service provider will provide documentation of applicable PCI DSS requirements to be maintained as part of the provided service, and submit a copy of their current *Attestation of Compliance*. The PCOC will maintain a program to monitor service providers' PCI DSS compliance status at least annually.

**4.8** In the event of a security breach on a UVU system or that of a service provider that handles UVU consumer payment card data, the Computer Incident Response Team (CIRT) shall oversee the investigation and remediation of issues that led to the breach. The CIRT is responsible for providing updates to University Administration and for ensuring that the card brands and acquiring banks are notified.

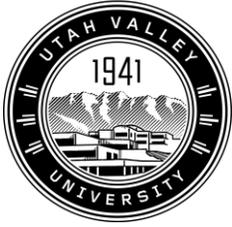
## 5.0 PROCEDURES

### 5.1 Payment Card Oversight Committee (PCOC)

**5.1.1** The oversight of PCI compliance throughout the University will be the joint responsibility of the Associate Vice President–CIO/Information Technology, Senior Analyst–PCI Security, Officer–Security/IT Services, Controller–Business Services, and the Senior Accountant of Treasury Services.

**5.1.2** The PCOC is responsible for:

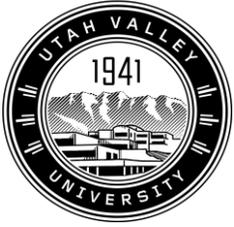
- 1) Monitoring the University's compliance with standards set by PCI SSC;
- 2) Assessing, analyzing, and providing information as required under the standards to merchant providers;
- 3) Granting the privilege of accepting payment cards to campus merchants (both university and non-university entities) and providing oversight of the merchant setup procedures to reduce the risk of exposing the University, the merchant entity, or the merchant entity's patrons to unnecessary information security risks; and
- 4) Coordinating training activities for the campus merchant community about their responsibilities regarding PCI compliance.



**5.2 PCI Security Breach Protocol**

**5.2.1** The events and circumstances of a suspected security breach must be immediately reported to the CIRT. The CIRT will immediately begin an investigation and follow the incident response plan, including identification, assessment, containment, eradication, recovery, and follow-up. During the process of responding to the incident, the CIRT team lead will ensure university administration is alerted and kept up-to-date, and will follow procedures for notifying card brands and acquiring banks.

<b>POLICY HISTORY</b>		
<b>Date of Last Action</b>	<b>Action Taken</b>	<b>Authorizing Entity</b>



**UTAH VALLEY UNIVERSITY**  
Policies and Procedures

Page 7 of 7