UTAH VALLEY UNIVERSITY
Policies and Procedures

POLICY TITLE	PCI DSS Compliance	**Policy Number**	457
Section	Facilities, Operations, and Information Technology	**Approval Date**	May 9, 2023
Subsection	Information Technology	**Effective Date**	May 9, 2023
Responsible Office	Office of the Vice President of Digital Transformation		

1.0 PURPOSE

1.1 The purpose of this policy is to help ensure that the University serves as an effective steward of personal financial information entrusted to it by its constituents; protects the privacy of its constituents; complies with the Payment Card Industry Data Security Standard (PCI DSS); and strives to avoid a security breach aimed at obtaining cardholder information.

1.2 To minimize inappropriate exposures, losses, and 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 Policy 445 *Institutional Data Management and Access*

2.3 UVU Policy 447 *Information Security*

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 that oversees the investigation and remediation of issues that led to a security breach of IT systems. The Information Security Officer oversees his group.

3.7 Merchant: For the purposes of the PCI DSS and this policy, 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 or services.

3.8 Payment Card Oversight Committee (PCOC): A group tasked with the oversight of the University's PCI DSS compliance. It comprises the Vice President of Digital Transformation or designee, the Controller, and others as appointed.

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

3.10 Primary account number (PAN): A 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 authorize payment-card transactions.

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 hosting providers and service providers that provide managed firewalls, IDS, and other services, as well as hosting providers and other entities. Entities that only provide communication links

without access to the application layer of the communication link, such as telecommunications companies, are excluded.

4.0 POLICY

4.1 UVU is responsible for its PCI DSS compliance and any 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 merchants that conduct business on university property or for security breaches that occur on non-university merchants' systems.

4.2 All merchants (both university and non-university) 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) and comply with the standards set by the PCI SSC.

4.3 As a condition of PCOC approval, University merchants shall provide adequate training for all employees dealing with payment card data on how this data should be handled securely and the risks associated with payment card data relevant to the scope of their employment duties. Merchants shall follow the information security procedures outlined by the PCOC.

4.4 To ensure proper handling and safeguarding of payment card information, merchants will work with the PCOC to have 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 merchants must complete the appropriate *PCI DSS Report on Compliance* or both *the Self-Assessment Questionnaire* and the *Attestation of Compliance*. These documents must be submitted to the Finance and Business Services Office annually by the last university working day in June.

4.7 Non-university merchants 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 that the service providers possess or otherwise store, process, or transmit on behalf of the University, 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 must submit a copy of their current *Attestation of Compliance*. The PCOC will maintain a program to verify 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 responsibility of the PCOC.

5.1.2 The responsibilities of the PCOC include the following:

5.1.2.1 Monitoring the University's compliance with standards set by PCI SSC;

5.1.2.2 Assessing, analyzing, and providing information as required under the standards to merchant providers;

5.1.2.3 Granting the privilege of accepting payment cards to campus merchants (both university and non-university) and providing oversight of the merchant setup procedures to reduce the risk of exposing the University, the merchant, or the merchant's patrons to unnecessary information security risks; and

5.1.2.4 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 reported immediately 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.

POLICY HISTORY		
Date of Last Action	Action Taken	Authorizing Entity
February 19, 2015	Policy approved.	UVU Board of Trustees
May 9, 2023	Revised policy approved.	UVU Board of Trustees