BOISE STATE UNIVERSITY

University Policy 6340

Payment Card Industry Data Security Standard (PCI DSS) Policy

Effective Date

April 2019

Responsible Party

Chief Financial and Operating Officer and Vice President for Finance and Operations, vpcfo@boisestate.edu

Scope and Audience

This policy applies to all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers and all other entities or individuals with access to University PCI systems and equipment, including those used by the University under license, contract or other affiliation agreement.

Additional Authority

- Payment Card Industry - Data Security Standard, ("PCI-DSS")
- University Policy 8060 (Information Privacy and Data Security)

1. Policy Purpose

To protect and preserve the privacy and security of Payment Card data while conducting University business operations.

2. Policy Statement

Boise State University is committed to protecting and preserving the privacy and security of Payment Card data while conducting University business operations. The focus of the Payment Card Industry Data Security Standard (PCI DSS) Policy is to protect against Payment Card fraud in e-commerce and terminal-based transactions. This policy defines and provides requirements and guidance for all Payment Card activities and establishes required practices for all members of Boise State University. The policy addresses access to Boise State University's computing and network resources with regard to payment card processing as well as any freestanding Payment Card processing unit or point-of-sale system.

3. Definitions

3.1 Cardholder

Person/agency to whom a card is issued or any individual authorized to use a card.

3.2 Cardholder Data

Primary Account Number (PAN) along with Cardholder name or expiration date or CVC2/CVV2/CID security pins.

3.3 Chief Information Security Officer (CISO)

The individual whose primary responsibility is the oversight of information security of University networks, systems and data.

3.4 Credit Card Processing

The act of storing, processing, or transmitting credit card data.

3.5 E-commerce Application

Any network-enabled financial transaction application.

3.6 Merchant

University unit that accepts Payment Cards using the University's merchant processor(s). Each Merchant is assigned a merchant identification number (MID) by University Financial Services.

3.7 Payment Card

Approved credit and debit cards used to make a payment.

3.8 Payment Card Industry Data Security Standard (PCI DSS)

Standard that all organizations, including online retailers, must follow when storing, processing and transmitting their customers' credit card data.

3.9 PCI Governance Committee

University stakeholders appointed by the Vice President and Chief Financial Officer that are tasked with managing PCI compliance across campus. Committee membership at a minimum will include the Associate Vice President of Finance and Administration, University Controller and the CISO.

3.10 POS Device

Point-of-sale (POS) computer or Payment Card terminals either running as stand-alone systems or connecting to University networks.

3.11 Restricted Data

Level 1 data as outlined in the University Data Classification Standard or any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protections whether in storage or in transit.

3.12 University Financial Services (UFS)

UFS is a unit within the Vice President and Chief Financial Officer organization. Student Financial Services, within UFS, handles customer support for eCommerce web pages and the Controller's office is responsible for reconciliation with the bank and other transactional activity.

3.13 Virtual Payment Terminal

Web-browser-based access to a third-party service provider website to authorize Payment Card transactions when the Merchant manually enters Payment Card data via a securely connected web browser. Unlike physical terminals, Virtual Payment Terminals do not read data directly from a Payment Card.

3.14 Web Development

The design, development, implementation, and management of the user interface of the E-Commerce Application such as portable API code or redirect URLs.

4. Merchant Requirements

Requirements for Merchants using a Payment Card terminal, as well as Merchants processing or transmitting transactions using e-commerce, are as follows:

a. Terminal transactions include face-to-face transactions using a network connection, a phone line (where necessary) or cellular terminals. In some cases, a terminal's keypad may be used to enter card-not-present transactions where Cardholder Data was received via postal mail or over the phone.

b. E-commerce transactions include, but are not limited to, the following:

- Links on University websites redirecting individuals to another payment processing website;
- Point-of-sale transactions at a computer cash register using PCI payment applications, including point-of-sale software on a computer, to transmit, process or store Cardholder Data;
- Use of a third-party vendor Virtual Payment Terminal to transmit Cardholder Data;
- Approved payment processor Application Processing Interface (API) utilizing iFrame technology.

5. Payment Card Processing and Approval Management

a. Boise State University strives to eliminate storing credit card information on University networks, workstations or mobile devices.

b. All Boise State University divisions and departments desiring to accept payment for financial transactions electronically via the Internet using e-commerce are required to process all transactions through gateways approved by University Financial Services.

c. Methods for accepting Payment Cards may be found on UFS's website. These have been approved by UFS and are required regardless of the transaction method used (e.g., e-commerce, POS Device or e-commerce outsourced to a third party).

d. All technology implementations (including approval of authorized payment gateways) associated with the Payment Card processing must be in accordance with the PCI DSS

Policy and be approved by OIT and the University Controller prior to entering into any contract or purchasing software and/or equipment.

e. Tasks including, but not limited to, faxing, emailing, and scanning payment forms; maintaining spreadsheets, receipts or documents in electronic or written form; and using messaging technology are prohibited if they include Cardholder Data.

f. Terms and conditions between third-party vendors and the University must address the protection of Cardholder Data in adherence with the law, University policies, and PCI DSS standards.

6. Payment Card Maintenance Standards and Responsibilities

a. All members of the University community share the responsibility for protecting information and data with which they are entrusted. Departments that manage Payment Card transactions must adhere to the strict requirements of this policy and of the PCI DSS standards.

b. All Cardholder Data should be classified as Restricted or Level 1 as outlined in the University Data Classification Standard.

c. Access to Payment Card processing systems and related information must be restricted to appropriate personnel. In some cases, personnel may be subject to background and credit checks prior to participating in the processing of credit card payments. It's the department's responsibility to ensure that all employees involved in e-commerce or POS transactions understand all requirements as outlined in the PCI DSS Policy.

d. All individuals who handle, transmit, support or manage Payment Card transactions received by the University must complete the University PCI training upon hire and annually thereafter as identified by their supervisor. PCI training modules are available through the CISO Cybersecurity Training Department.

e. All, in scope, PCI network infrastructure and POS Devices will be administered in accordance with the requirements of the PCI DSS standards.

f. The Office of Information Technology will strive to maintain and enforce secure network infrastructure University-wide in accordance with the requirements of current PCI DSS standards.

g. The CISO or authorized designate in collaboration with University Financial Services will inform current Merchants of changes to applicable policies, laws, regulations and industry standards.

h. Each department responsible for Payment Card processing may be subject to an Annual Self-Assessment Questionnaire as determined by the CISO or authorized designate.

i. Third parties providing payment gateways or who interact in any way with Payment Cards as a form of payment must provide an Attestation of Compliance for PCI-DSS compliance annually.

j. Only approved Boise State University logos may be used on e-commerce sites associated with the University.

7. Reporting Security Standards

Protecting data is everyone's responsibility. Known, suspected and alleged incidents involving lost, disclosed, stolen, compromised or misused Cardholder Data must be reported per the Boise State Incident Response Procedure.

8. Compliance

a. Failure to comply with the PCI DSS Policy and the above-referenced requirements will be deemed a violation of University policy and may result in suspension of electronic payment capability for the affected department.

b. It is the responsibility of all individuals to whom this policy applies to be informed of and follow the requirements under this policy to protect Cardholder Data.

c. Violations of this policy will be handled consistent with University disciplinary procedures applicable to the relevant individuals or departments. Appropriate sanctions include, but are not limited to, termination of the relationship and/or potential criminal prosecution under applicable federal, state and local laws. Should Boise State incur monetary fines or other incidental expenses from security breaches or regulatory infractions, the University may recoup these costs from the non-compliant department, school or auxiliary organization.

d. Technology that does not comply with current PCI-DSS standards will be disconnected from network services.

e. Boise State University 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.

9. Related Information

Boise State Incident Response Procedure:
https://www.boisestate.edu/oit/itgrc/it-plans-procedures/it-incident-response-procedure/

PCI Compliance
https://www.boisestate.edu/vpfa-treasury/pci-compliance/

University Data Classification Standard:
https://www.boisestate.edu/oit/itgrc/it-standards/data-classification-standards/

Last Review Date

August 25, 2021