Payment Card Industry Data Security Standards (PCI DSS) Compliance Policy

Effective Date: November 6, 2019

PURPOSE:

Georgia State University ("University") is committed to developing, adopting, and maintaining appropriate information security policies, standards, and procedures to ensure integration of information security with the University's mission, business strategy, risk posture, and in accordance with applicable legal and regulatory guidelines.

The Payment Card Industry (including, but not limited to, American Express®, MasterCard®, VISA®, and other major credit card issuers) has established important and stringent security requirements to protect credit/debit card data. These requirements are called the Payment Card Industry Data Security Standards ("PCI DSS"). The PCI DSS provides standards for safeguarding credit/debit card data for all card brands and details the security requirements for transmitting, storing, accessing, and processing personally identifiable data associated with a cardholder, including, but not limited to, name, address, social security number, account number, and expiration date (collectively, Cardholder Data").

This PCI DSS Policy focuses on safeguarding credit/debit data and Cardholder Data and requires University policies and procedures as it relates to credit/debit cards to be in compliance with PCI DSS requirements. This Policy does not address federal, state, or other applicable laws and regulations that may apply to payment card transactions.

SCOPE:

This Policy applies to any University unit or department that has access to Cardholder Data (each such unit or department hereinafter referred to as "Campus Merchant") and to the people, processes, and technology that handle Cardholder Data at or on behalf of the University. Specifically, this Policy applies to any University unit or department, cooperative organization, employee (full-time, part-time, and temporary), student, volunteer, service provider, vendor, or other person or entity that processes, transmits, or stores Cardholder Data in a physical or electronic format for the University or using University resources or that has access to the University Cardholder Data environment. All technical and operational system components, including software, computers, and wired or wireless electronic devices, involved in processing Cardholder Data, whether owned or leased by the University, are subject to this Policy.

This Policy does not apply to individuals' use of credit cards, including procurement cards ("P-Cards"), or any other such instance where University units or departments are not collecting, processing, transmitting, or storing credit/debit card data or Cardholder Data.

POLICY:

All Campus Merchants must be (a) approved by the University's PCI Team (as defined below); (b) comply with the PCI DSS; and (c) comply with Georgia State University Credit Card Processing Procedures (as defined below).

Any University unit or department that seeks to process credit/debit card data and have access to Cardholder Data must follow the process set forth below:

1. A University unit or department shall submit an ITS Help Desk ticket to initiate the application process. The unit or department must provide:

    a. sufficient information about its plan to process credit/debit cards and its planned transaction method for processing credit/debit cards (i.e., online/e-commerce, Point-of-Sale ("POS") device, or e-commerce outsourced to a third-party service provider (e.g., TouchNet®));

b. a designated full-time University employee who will have primary authority and responsibility for ensuring the unit or department's compliance with PCI DSS and the Georgia State University Credit Card Processing Procedures (such individual shall hereinafter be referred to as the "Campus Merchant Representative"). The Campus Merchant Representative, whose full list of duties can be found in the Georgia State University Credit Card Processing Procedures, shall also be responsible for ensuring that all applicable unit or department personnel undergo annual PCI DSS training and for providing an annual attestation that the unit or department is compliant with this Policy.

2. The University's PCI Team shall promptly review the request and work with the unit or department to ensure that all PCI requirements and procedures are satisfied by the unit or department. The PCI Team shall be comprised of representatives (or their designees) from the University units: (1) Office of the Comptroller; (2) Office of the Chief Information Security Officer ("CISO"); and (3) the University's PCI Internal Security Assessor ("PCI ISA").

3. If a unit or department's proposed credit/debit card processing involves processing credit/debit cards through a third-party, such third-party (and its policies and procedures) must be reviewed by the PCI Team to ensure compliance with PCI DSS.

4. If the PCI Team approves the unit or department's plans, the unit or department shall submit any contracts or agreements for services (e.g., e-commerce Terms and Conditions, contracts to support POS devices, etc.) through the University's contract routing process, including, but not limited to review by the University's PCI ISA, the Office of Procurement, and the Office of Legal Affairs.

5. Following approval from the PCI Team and obtaining a fully executed contract or agreement for services signed by an authorized representative of the University, a unit or department may begin processing credit/debit cards.

ENFORCEMENT:

Violations of this Policy could result in a Campus Merchant's loss of access privileges to the University network and data, and/or for individuals/service providers, disciplinary action, up to and including termination of employment and/or termination of contracts with the University. Additionally, if applicable, certain violations may be referred to the appropriate legal authorities for criminal prosecution.

Policy Administration	
Responsible Office(s)	Office of Finance & Administration, Accounting Services 75 Piedmont, Citizens Trust Bldg. Suite 1200 Atlanta, Georgia 30303 404-413-3071 Instructional Innovation and Technology (IIT) Cybersecurity 34 Broad Street, NE Suite 1300 Atlanta, Georgia 30303 security@gsu.edu 404-413-4378
Responsible Executive(s):	Bruce Spratt, Comptroller

	Phil Ventimiglia, Chief Information Officer Ren Flot, Chief Information Security Officer

Policy Management	
Policy History Approval Date: Approving Body (if applicable):	 November 6, 2019 Administrative Council

RELATED POLICIES, STANDARDS, GUIDELINES:

GSU Credit Card Processing Procedures

REFERENCES:

Security Standards Council (Payment Card Industry Security Standards)
PCI-DSS Quick Reference Guide