Title: **Payment Eligibility and Standards for Processing of Payment Cards Policy**	**Policy Category:** **Financial**
Issuing Authority: **Administration & Finance**	**Responsibility:** **Administration & Finance**
Publication Date: **11/16/2022**	**Next Review Date:** **11/16/2025**

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

Policy Statement/Background:

Stony Brook University is committed to safeguarding Personally-identifiable Information and payment card data. In an effort to help assure anyone using a credit card, debit card or Wolfie-Wallet when conducting business with the University or Campus Merchants, the University is committed to upholding and adhering to the Payment Card Industry Data Security Standards Council issued standards (PCI DSS) to all activities associated with processing these cards.

Scope

All units of Stony Brook University intending to accept Payment Cards to conduct business, all Campus Merchants, any individual having access to cardholder data, and to the people, processes and technology that handle cardholder data at or on behalf of Stony Brook University (collectively referred to herein as "Campus Merchants").

Policy:

The University is committed to safeguarding Personally-identifiable Information, including Cardholder Data. The privilege of accepting Payment Cards at the University depends upon strict adherence to the PCI DSS — which are specified security standards. The PCI DSS must be adhered to for all types of Payment Cards processed by Campus Merchants. Cardholder Data is not to be collected by or stored in campus-based systems or files. PCI Certified Service Providers are to be used instead.

The Chief Information Officer (CIO) will develop and maintain a Cardholder Data Environment (CDE) in order to support this policy. The CDE must be used by any Campus Merchant that retains or processes data through campus-based systems.

Individuals, departments, third-party contractors, or organizations operating on campus or under the name of the University may only accept Payment Cards on campus or through the web when expressly authorized to do so by the University Controller, who will maintain an inventory of authorized Campus Merchants. The Office of the University Controller will issue guidelines and advisories from time to time which further define and clarify the obligations of Campus Merchants and the steps to be followed to be permitted to accept Payment Cards.

Education

The Student Financial Services Office will develop, maintain and offer training programs for personnel responsible for handling payment card transactions and related data.

Compliance

Campus Merchants must maintain compliance with issued University guidelines and the current version of Payment Card Industry Data Security Standards. They must assure that staff assigned to handle Payment Card transactions are vetted and trained in the proper handling of such data.

Any suspected loss or compromise of cardholder information must be reported immediately by sending an email containing a complete description of the incident to paymentcardcompliance@stonybrook.edu, the University Controller and the Information Security Office (information_security@stonybrook.edu). Upon receipt of a report of any such incident, these offices will take steps to research the incident and cause any problems to be remediated. Any suspected incident of payment card fraud should also be reported to University Police for investigation.

Any employees who fail to comply with this policy may be subject to disciplinary action, up to and including suspension/termination, in accordance with the applicable collective bargaining agreement. Campus Merchants who fail to comply are subject to having their Payment Card acceptance privileges revoked.

All contracts (including revocable permits) with external vendors that are to accept Payment Cards shall incorporate approved PCI language requiring compliance with this policy and adhere to guidelines issued by the University Controller. Responsibility for compliance, data loss, and fraud related to Payment Card transactions shall rest with the Third-Party Merchant.

Definitions:

Campus Merchant: Any individual or entity which provides services on behalf of Stony Brook University or its affiliates that uses payment card information to process transactions.

Cardholder Data: All personally identifiable data, including information printed on a Payment Card or stored on its magnetic stripe or chip and personal identification numbers entered by the Payment Card holder.

Cardholder Data Environment (CDE): A separate computer network that segregates Cardholder Data and processes.

Payment Cards: Credit Cards (M/C, Visa, Discover, AMEX), Debit Cards, and Wolfie-Wallet.

Payment Card Industry Data Security Standards (PCI DSS): A standard for handling Credit Cards formulated, issued, and enforced by the PCI Security Standards Council. While the standard applies to credit card processing this policy calls for the same processes, checks and controls to be applied to Debit Card and Wolfie-Wallet transactions.

PCI Certified Service Provider: Any company that stores, processes, or transmits cardholder data on behalf of another entity through services that have been certified as meeting Payment Card Industry Data Security Standards.

Personally-identifiable Information (PII Data): Refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual (see OMB Memorandum below).

Third-Party Merchant: Any contractor or subcontractor acting as a Campus Merchant.

Contact:

Additional information about this policy is available here:

Jeffrey Mackey
Director for Finance Policy, Compliance and Internal/System Controls
Stony Brook Union, Suite 207-06
Stony Brook, NY 11794
(631) 632-9583
Financepolicyandcompliance@stonybrook.edu

Relevant Standards, Codes, Rules, Regulations, Statutes and Policies:

- PCI Data Security Standard, Version 4.0
- OMB Memorandum M-07-16