|  |  |  |
| --- | --- | --- |
| HYPERLINK "https://www.bentley.edu/offices/information-security-and-data-privacy/bentley-university-pci-dss-policy" PCI DSS Policy |  |  |
| Policy Owner  Finance & Administration  Associated Policy:  [PCI DSS Policy](https://www.bentley.edu/offices/information-security-and-data-privacy/bentley-university-pci-dss-policy) | Policy Contact  Cashier | Date Revised:  6/1/2022  Effective Date:  6/1/2022 |
| Policy StatementAll acceptance of payments via payment cards, including e-commerce, on behalf of the University requires the prior approval of the Controller and must comply with current PCI DSS, as well as with all applicable legal, regulatory and University policy requirements, in order to protect cardholder data and to protect the University from risk. No department, organization, employee, contractor or agent is authorized to process Internet-based payment transactions, credit or debit card payments or electronic funds transfers without prior approval from the Controller.The University’s policy is to outsource all processing of payment card transactions to a University-approved PCI-compliant Third Party Processor to the extent possible. The University does not capture, store or transmit cardholder data electronically on any network-connected computer or device. Departments may store only the last four digits of a card number.Reason for Policy Cardholder data is high-risk confidential information that is protected by state and federal law and the University has a legal obligation to protect it. The major payment card companies (MasterCard, Visa, Discover, American Express and JCB) require all merchants to follow Payment Card Industry Data Security Standards (“PCIDSS”) designed to prevent cardholder fraud and identity theft.  In addition to PCIDSS, credit and debit card account numbers are subject to regulation under M.G.L. 93 H, 93 I and 201 CMR 17.00 (the “Massachusetts Data Privacy Laws and Regulations”) and are considered Sensitive Personal Information (SPI).  The risks of non-compliance by the University include substantial fines and penalties imposed by the card associations, liability for financial losses incurred as a result of a security failure, and damage to the University’s reputation. This Policy Applies To This policy applies to any Bentley department, organization, employee, contractor or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of payment card and e-commerce payments. Contracts with third parties that accept payment cards on behalf of the University must contain terms consistent with this policy and must be approved in advance by Procurement and Finance & Administration. | | |

# Procedures

In the course of doing business at Bentley University, it may be necessary for a department to accept credit cards for payment. The opening of a new merchant account for the purpose of accepting and processing credit cards at the University is done on a case by case basis and coordinated through Finance & Administration operations. Any fees associated with the acceptance of the credit cards in a department will be charged to that department.

Any department that seeks to accept credit cards or electronic payments must submit a request form to Cashier Services. No University unit, department or employee may contact a credit card processor (PayPal, Stripe) and/or social media (Facebook, Twitter) directly to obtain access to credit card privileges for University business needs.  The sale of goods and services to entities outside the university community may raise special considerations (e.g. unrelated business tax, accounting or legal issues, etc). Any new sales should be reviewed by the Controller.

Any department accepting credit cards on behalf of the University must designate an individual within the department who will have primary authority and responsibility within that department for credit card transactions and compliance with all regulations.

Specific details regarding processing and reconciliation will depend upon the method of credit card acceptance and type of merchant account. Detailed instructions will be provided by Finance and Administration operations when a new merchant account is opened.

# Definitions

**Authorized Vendor**: a PCI DSS-compliant vendor.

**Cardholder Data**: payment card components that are required to be protected, including primary account number, cardholder name, expiration date, service code, card verification code, full magnetic strip data and PIN.

**E-commerce**: buying and selling of products or services over the Internet.

**Merchant**: an entity that accepts payment cards for goods and services.

**Payment Card**: includes both credit cards and debit cards.

**PCI DSS**: The Payment Card Industry Data Security Standards are policies and procedures mandated by the major card companies (MasterCard, Visa, American Express, Discover and JCB) and intended to optimize the security of card transactions and protect cardholders against misuse of their personal information.

**Self-Assessment Questionnaire (SAQ)**: A questionnaire merchants are required by PCIDSS to complete annually to validate their compliance with PCIDSS.

**Third Party Processor**: an entity to which credit card transactions are outsourced by the University for processing. Third parties are contractually required to adhere to PCIDSS requirement and acknowledge they are responsible for security of cardholder data.