Last Reviewed: November 2023

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

1. Scope and Purpose

This policy pertains to all Bentley units and personnel that participate in credit and debit card processing. It requires them to have documented procedures that comply with the provisions and requirements of the Payment Card Industry Data Security Standard (PCI-DSS) for collecting, processing, transmitting, storing, and disposing of cardholder data (CHD). The PCI-DSS is intended to mitigate the risks of identity theft and financial fraud associated with payment card use.

2. Definitions

Cardholder data (CHD) – Any personally-identifiable data associated with a cardholder. Such data include account number, expiration date, name, address, social security number, Card Validation Code, Card Verification Value, Card Identification Number, or Card member ID

- **PCI-DSS** - Payment Card Industry Data Security Standard
- **Merchant** – Organization that collects payments by credit or debit card (i.e., the University or one of its departments)
- **Merchant account** – Number assigned to the merchant by the bank that processes its payment card transactions
- **CISO** – Chief Information Security Officer

3. Credit Card Acceptance and Processing

The opening of a new merchant account for the purpose of accepting and processing credit or debit cards at the University occurs on a case by case basis, only after careful consideration by designated University officials and preapproval by the Vice President and Chief Financial Officer (CFO)/Treasurer or his/her designee.

Any fees associated with the acceptance of the credit cards in a department will be charged to that department.

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 maintaining required procedures for credit and debit card transactions.

Specific details regarding processing and reconciliation will depend upon the method of credit or debit card acceptance and type of merchant account. Detailed instructions will be provided by the Financial Operations director designated by the Associate Vice President for Finance when a new merchant account is opened.

4. Credit Card Data Security

Departments that handle or store cardholder data (CHD) must have the following components in their CHD handling procedures and ensure that these components are in place and maintained on an ongoing basis.

- Restriction of CHD access only to those users who need the data to perform their jobs
- Maintenance of a list of department employees with access to CHD and review of the list annually and when there is a change in staff, to ensure that the list reflects the most current access needed and granted
- Protection of CHD, whether collected on paper or electronically, against unauthorized access
- Security against unauthorized use for all equipment used to collect CHD in accordance with the latest PCI-DSS version
- Physical security controls to prevent unauthorized individuals from gaining access to the rooms or cabinets that store the equipment, documents, or electronic files containing CHD
- Training and, if appropriate, background checks of all personnel, including staff, students, and volunteers, who handle CHD
- Due diligence procedures to ensure that all vendors and other third parties who handle CHD and processing on the University's behalf comply with requirements of PCI-DSS
- Quarterly scans of any servers that store or transmit CHD by an Approved Scanning Vendor (ASV) qualified by the PCI-DSS Council
- Prohibition against using non-secure channels such as email, Instant Messaging (IM), or Social Media to transmit CHD or as a method to supply such information; and, in the event that this prohibited use does occur, disposal and/or reporting as outlined in sections 5 and 6
- If a fax machine is regularly used to transmit credit card information to a merchant department, provision of a stand-alone machine with no other purpose and with physical security commensurate with the security provided to paper records that contain CHD; and disposal of faxed CHD according to the requirements outlined in section 5
- Prohibition against storing full credit or debit card numbers, the full contents of any track from the magnetic stripe, or the card-validation code on any Bentley-owned database, electronic file, or other electronic repository of information
- Prohibition against using Bentley-issued or personally-owned computers and electronic media devices to store CHD. Examples of these devices include, but are not limited to,

desktops, laptops, CDs, DVDs, USB flash drives, smartphones, tablets, and portable external hard drives.

5. Data Retention and Destruction

- CHD in paper form must be stored in a physically secure location, for no more than three months for reconciliation purposes or, in very limited situations by donor request for longer periods, and destroyed immediately following the required retention period.
- The department is responsible for maintaining a regular schedule for deleting or destroying CHD to ensure none is kept beyond applicable record retention requirements.
- Paper documents containing CHD must be shredded in a cross-cut shredder.
- Electronic data must be sanitized with an electronic shredding tool sponsored by the University.

6. Responding to a Data Security Breach

Anyone with knowledge or suspicion of a security breach is instructed to report the incident immediately to the Bentley Help Desk (helpdesk@bentley.edu or 781-891-2854) and the CISO (cybersecurity@bentley.edu). If warranted, the University will invoke its Cybersecurity Incident Response Plan with further notifications and procedures.

7. Responsibilities for Compliance

PCI-DSS compliance at Bentley is a joint effort among all departments associated with collecting payments to Bentley by means of credit and debit cards. The Vice President and CFO/Treasurer is responsible for PCI compliance, with support from the Controller and CISO. These offices work jointly to ensure that the departments who process CHD are PCI-compliant. They also attest to merchant bank(s) regarding the University's PCI compliance. Individual departments are responsible for the compliance of their personnel, procedures, applications, point-of-sale devices, and departmentally administered systems that process or transmit CHD. Departmental representatives will be required to participate in periodic PCI compliance audits and implement any procedural or system changes that may be required by the Vice President and CFO/Treasurer upon recommendation by the CISO, internal auditors, or external auditors.

8. Exceptions and Enforcement

Any exceptions to this policy are to be reviewed and approved by the Vice President and CFO/Treasurer or his/her designee, in consultation with the CISO.

Failure to meet the requirements outlined in this policy may result in suspension of the physical and, if appropriate, electronic payment card collection capability for affected departments. As described in Bentley's Acceptable Use Policy, anyone found to have violated this policy may be subject to disciplinary action, up to and including immediate termination.

9. Policy Support Contacts

Controller

Chief Information Security Officer (cybersecurity@bentley.edu)

10. Supporting Documentation

Acceptable Use Policy

Cybersecurity Incident Response Plan

Record Retention Schedule

Revision History

Version	Date	Author	Reviewers	Approvers	Notes
1.0	7/01/2018		Vice President and CFO	Vice President and CFO	Policy created
1.1	11/10/2023	David Norman			Updated links and revision history on policy