CUSTOMER PAYMENT CARD DATA POLICY

CUSTOMER PRIVACY

In accordance with the Payment Card Industry Data Security Standards (PCI DSS), Gramm-Leach-Bliley Act (GLBA) and PTC Policy, the only approved mechanisms used in processing credit card transactions electronically are as follows:

1. Enable clients to use Self-Service options, so the department is not processing credit card transactions on their behalf:
2. Utilize PTC's payment gateway where appropriate
3. Use an alternate payment gateway, which utilizes the campus's PCI DSS compliant network instead of the general-purpose network, and is approved by the IT Department
4. Utilize an IT Department authorized Point-of-Sale (POS) device that connects to an authorized cellular network

Compliance with PCI DSS is required of all PTC employees, contract workers, including student workers, and departments that accept, process, transmit or store payment cardholder data. Only PTC employees, contract workers, including student workers who are adequately trained, may accept and/or access cardholder data, devices, or systems which store or access cardholder data. Only PCI DSS compliant equipment, systems, and methods may be utilized to process, transmit, and/or store cardholder data. Similarly, third-party vendors utilized by the college must provide evidence of annual PCI compliance both prior to entering into a contract, and on an annual basis thereafter. Do not email credit card data or other PII on the IT network.

The transmission of an individual's PII including credit card data, over the system for non-business reasons, is prohibited. In addition, PTC prohibits employees, including contract and student workers, from processing any credit card transactions on behalf of customers using the PTC network (both wired and wireless connections). This restriction also applies to third-party organizations, vendors, and service providers operating on campus. Credit card transactions on behalf of customers using any PTC-issued workstations (desktop, laptop, tablet, mobile device) or personal devices are prohibited.

The actions and circumstances of a suspected security breach that could negatively affect cardholder data or the PTC's compliance with PCI DSS must be immediately reported and investigated in accordance with college policy. Vendors

and service providers operating on campus that accept credit cards must execute a contract addendum affirming evidence of their annual compliance with PCI DSS. Non-PTC employees who are acting on PTC's behalf must comply with PCI DSS, and provide yearly evidence therein.