Baylor ITS provides several mechanisms for conducting eCommerce. Those systems are critical components of Baylor University's IT infrastructure: handling large numbers of transactions and large amounts of money. Baylor's eCommerce systems are selected, managed and implemented:

- to solve specific business challenges, and
- to meet particular standards in terms of security and risk management.

Baylor ITS commits to the following standards and procedures and will work to insure the broadest application of these across the university. (Some of these statements may be redundant or overlap. However, they are included here so as to make clear Baylor ITS'; intent.)

1. Unless special provisions are made, Baylor ITS will only support eCommerce conducted on Baylor University's accounts. All merchant accounts will be under the control of Baylor University or University-owned related entities and managed by Baylor University Financial Services. Baylor ITS will not develop or support eCommerce for merchant accounts that belong to or are managed by a third party.

2. All transmission of sensitive financial data (e.g. credit card numbers, bank account numbers, etc.) will utilize SSL in order to encrypt the data while in transit across networks.

3. Baylor will comply with all PCI DSS standards in the course of conducting eCommerce.

4. Baylor requires that third party software be PA DSS compliant. Where Baylor writes or commissions software development, all software will be PA DSS compliant.

5. Beyond PCI DSS and PA DSS, Baylor ITS is committed to an approach where the handling, processing, and storage of the data required to facilitate eCommerce (especially credit card and bank account numbers) will be handled by secured off-site third party servers. This means that Baylor intends that credit card and bank account numbers never pass through any Baylor written programs or be stored (even temporarily) on Baylor owned or controlled servers.

6. Prior to enabling any eCommerce application (prior to processing any transactions) Baylor ITS will require clear notice from the Baylor Tax & Compliance Accounting office as to any requirement to collect sales tax. Further, Baylor ITS will rely upon the Tax & Compliance Accounting office to make any determination as to other tax implications of putting a transaction online.

7. Baylor University is not a retail merchant. Therefore, Baylor ITS does not create or maintain systems that are typically used in support of retail eCommerce. The systems to insure compliance with laws related to timing for acceptance of payment in relation to shipment of goods, sales tax collection, order fulfillment, shipping cost calculations, and more simply are not within the scope of Baylor ITS to support. Therefore, Baylor ITS will not support the sale of material goods (e.g. a t-shirt, a book or a DVD) via eCommerce when that sale will require shipping the product. Sales of materials that are for pickup on campus may in some cases be supported. The risks and challenges are simply too great.
8. ITS will not endorse or support departments in contracting with third party vendors for eCommerce solutions. Any attempt to use an external system must be cleared by General Counsel and Cashiers regardless of the volume/value of transactions involved.

This guideline should not be construed such that every request for eCommerce can be met with Baylor's current systems. Because Baylor's eCommerce systems were selected and implemented to solve specific business challenges, it is possible that some requests or needs for eCommerce cannot be met with the current systems.

These guidelines will in no way diminish or reduce any other University policies or ITS guidelines. These guidelines should be viewed in light of an in addition to other University policies and ITS guidelines.

Rationale for Guideline

The movement of commerce to the Internet brings tremendous opportunities in terms of efficiency, geographic reach, and ease of use for both consumers and merchants. However, this move also brings a number of challenges and risks. The intent of these guidelines is to outline steps that will mitigate Baylor's risks with regard to eCommerce. These risks include the following:

- Identity theft;
- Non-compliance with industry regulations (PCI DSS and PA DSS); and
- Non-compliance with local, state, or federal laws (including tax laws).

(Note: While Baylor University is a non-profit corporation and enjoys certain exemptions for taxes, when Baylor acts as a merchant for the sale of many goods we are still required to collect and remit sales taxes. This is a complicated area of the law and accounting. Moving transactions to the Internet further complicates this situation for the university.)

Scope of Guideline

As the title of this guideline indicates, the scope of this guideline is to address eCommerce (see definitions) where Baylor is the merchant. Although some of the principles from this guideline may apply, Point of Sale (see definitions) transactions are not covered in this guideline. Further, for the purposes of this guideline, authorizations for payroll deduction are not considered to be eCommerce.

Definitions

**eCommerce**: Abbreviation for electronic commerce. eCommerce is the activity of buying or selling of products on online services or over the Internet. For the purposes of this document eCommerce is specifically the payment component of the interaction. Further, eCommerce for the purpose of this document involves the use and transmission of information permitting the merchant to receive funds directly from a financial institution (bank account number, credit card number, etc.). Authorization for payroll deduction is not eCommerce for the purposes of this guideline.¹

**PCI DSS**: Abbreviation for Payment Card Industry Data Security Standard. [PCI DSS are the] security procedures from the PCI Security Standards Council for merchants that accept credit cards online. It includes guidelines for user authentication, firewalls, antivirus, encryption, truncating account numbers, programming maintenance and vulnerability testing.²
PA-DSS: PA-DSS is the [PCI Security Standards Council]-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP). The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements. The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data and/or sensitive authentication data, in accordance with the PA DSS requirements document.

SSL: Abbreviation for Secure Sockets Layer. [SSL is] the leading security protocol on the Internet. Developed by Netscape, SSL is widely used to do two things: to validate the identity of a Web site and to create an encrypted connection for sending [or transporting] credit card and other personal data.

Point of Sale: Capturing data at the time and place of sale. Point of sale systems use computers or specialized terminals that are combined with cash registers, bar code readers, optical scanners and magnetic stripe readers for accurately and instantly capturing the transaction.

Adopted July 2009.
Modified May 13, 2019

1 eCommerce definition is copied from Wikipedia. ("E-Commerce."; Wikipedia, Wikimedia Foundation, 2 May 2019, en.wikipedia.org/wiki/E-commerce.)

2 PCI DSS definition is copied from the preamble to the PCI DSS entry in the PCMag.COM online encyclopedia. (http://www.pcmag.com/encyclopedia_term/0,2542,t=PCI+DSS&i=59104,00.asp)

3 PA DSS definition is copied from the PCI Security Standards Council's web site. (https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

4 The PA DSS requirements document (https://www.pcisecuritystandards.org/documents/PA-DSS_v3.pdf)

5 SSL definition is copied from the preamble to the SSL entry in the PCMag.COM online encyclopedia. (http://www.pcmag.com/encyclopedia_term/0,2542,t=SSL&i=51944,00.asp)

6 Point of Sale definition is copied from the preamble to the PCMag.COM online encyclopedia. (http://www.pcmag.com/encyclopedia_term/0,2542,t=point+of+sale&i=49444,00.asp)