Sanford School of Public Policy
Data Security and Security Awareness Policy and Procedures for Ecommerce Web Sites
Revised November, 2021

Background: Initial

Payment Card Industry Data Security Standard (PCI-DSS)
The credit card industry has implemented the **Payment Card Industry Data Security Standard (PCI-DSS)** to protect its customers, and compliance is required of all merchants and service providers that store, process, or transmit cardholder data. PCI-DSS is designed to safeguard sensitive data for all card brands. This Standard is a collaborative result between Visa, MasterCard, and other card companies, and is designed to create common industry security requirements. The standards are located at pcisecuritystandards.org/

Scope:

Any Sanford School business manager or designee wishing to process credit card payments online must adhere to this policy. This extends to the access of any reporting data that may be downloaded for reconciliation to a local secure server.

Purpose:

This document serves as the Internal Security Policy and Awareness Program Documentation required by Duke University for PCI-DSS compliance.

Policy:

Duke University Authority for PCI-DSS: Senior management for Duke University and Duke University Health System has confirmed Duke's E-Commerce department within Treasury and Cash Management as the central organizational structure to govern and enforce PCI-DSS compliance. Duke University's IT Security Office will be the authoritative source for the technical requirements associated with PCI-DSS. The E-Commerce department will lead all PCI-DSS efforts and will partner with the IT Security Office to determine appropriate technical compliance strategies. Specific requirements are located at https://finance.duke.edu/banking/ecommerce/reginfo.php. DKA

ALL Duke credit card merchants must comply with the PCI-DSS to ensure the security of cardholder data processed by their merchant account. Merchants must preserve the security and confidentiality of card numbers and cardholder information. It is PROHIBITED by Duke for any merchant to store full credit card information (16-digit account numbers (PAN), CV codes, PINs, or full magnetic stripe) on Duke systems and/or servers. DKA

All Duke University employees are required to sign the Duke Confidentiality agreement and a copy of this form is on file with the department HR office. A copy of this form is located at hr.duke.edu/sites/default/files/atoms/files/Confidentiality%20Agreement.pdf. DKA

All computers that are connected to network ports in the Sanford School are subject to Duke University Security Policies; this includes computers purchased with Duke funds and personal funds. These policies are located at security.duke.edu/policies-procedures. DKA

Ecommerce merchants are required to review Duke's E-Commerce requirements located at finance.duke.edu/banking/ecommerce/index.php. DKA

If the merchant or their designee needs to download data from the Cybersource business center, the data must be saved to password restricted portion of a network drive in order to provide maximum security of that data. *Note that the data available for download will only contain the last 4 digits of the cardholder number.* DKA

Security Awareness:

All Sanford School business managers or designees must take the annual "Duke University Security Awareness Training for Credit Card Processing" offered through the Duke LMS.

All Sanford School business managers or designees will subscribe to the DukePay Listserv to ensure they receive any important service notifications and other information regarding your e-commerce account. DKA

This policy may be periodically updated and all current online merchant account users will be notified of the changes via email and required to sign a copy of the amendments or new policy statement. DKA

An annual review of this document, which includes a review of the Sanford PCI Data Security and Security Awareness Policy web page, will be required by any user with access to an online merchant account with Cybersource. This page is at https://inside.sanford.duke.edu/wp-content/uploads/2020/10/Sanford-PCI-DataSecurity-Policy.doc. DKA DKA

Sanford School Business Manager or Designee for:

Sanford School of Public Policy

Center / Department / Store Name

David K Arrington

Print Name

Signature

11/03/2021

Date