



Date: November 2, 2022

To: CFBA members and UBC merchants

From: UBC PCI Working Committee

Re: Payment Card Industry Data Security Standards (PCI DSS)

The UBC PCI Working Committee would like your continued support and assistance in maintaining adherence to PCI DSS requirements across the University.

Breaches of security over customer information may lead to financial loss and/or damage the University's reputation. UBC is doing its part to protect itself from financial loss and/or loss of public confidence. The UBC PCI Working Committee aims to ensure that all existing merchants throughout UBC are compliant with PCI DSS, as well as any parties who plan to accept credit card as part of their business process.


PCI DSS is an externally driven mandate from the Payment Brands (i.e. Visa, MasterCard, Amex, JCB and Discover) imposed on all merchants accepting credit cards for payment of goods or services. The Payment Brands jointly developed PCI DSS to ensure that credit card customer information is adequately protected and to protect the credit card industry. The purpose of the PCI standards is to deter payment card fraud and to maintain a secure credit card environment. Every organization that stores, transmits or processes cardholder data must comply with the PCI DSS, that is enforced by the "acquiring bank", which are those organizations through whom the merchants may obtain a merchant account.

Merchants are required to undertake compliance validation of their cardholder data environment annually in accordance with the PCI DSS standards. The compliance procedures are typically composed of a vulnerability assessment scan and the audit of card data environment. MNP, who is UBC's Qualified Security Assessor (QSA), will be carrying out reviews of PCI DSS implementations to validate the compliance status of our merchants. UBC as a merchant is bound to follow and adhere to the PCI DSS policies and report its PCI DSS status to the Comptroller General of BC.

Before a merchant can start any credit card processing, all UBC PCI requirements must be adhered to. Use of UBC bank accounts require approval as per Resolution #2 and authorization will not be provided until the PCI requirements are met. Any incoming funds from a credit card Service Provider will not be credited to the UBC department (merchant) until PCI compliance is ensured. All merchants should contact Raul Ramos (rramos@mail.ubc.ca or 604-822-0259) for guidance in completing the applicable PCI requirements.

Please forward to the appropriate staff within your department/faculty.

Sincerely,



Holly Shepherd

Director, Treasury

PCI Working Committee Chairperson

On behalf of the UBC PCI Working Committee:

Mary Carmichael	Director, Internal Assurance
Larry Carson	Associate Director, Information Security Management
Michael Lonsdale-Eccles	Director, PRISM SRS, Risk Management Services
Sharon Rashtian	Associate Director, Security, Data, Access and Reporting
Chen Shi	Manager, Treasury Accounting
Chris Yong	PCI Technical Resource, Director, SHCS IT