# CREDIT CARD SECURITY POLICY – RECEIVING PAYMENTS

| | |
|---|---|
| **Section** | Treasury – Finance |
| **Contact** | Chief Finance Officer |
| **Last Review** | August 2022 |
| **Next Review** | August 2027 |
| **Approval** | SLT 16/08/164 |
| **Effective Date** | August 2022 |

## Purpose:

To ensure all credit card payments received on behalf of Massey University adhere to the requirements of the Payment Card Industry Data Security Standards (PCI DSS).

## Introduction:

- Credit cards are one of the preferred methods of payment for many students paying for tuition and non-tuition fees, and for other external parties paying for a variety of goods and services.
- Online credit card payments must only be processed through the University Online Payment Gateway. This integrates with the University's bank solution provider to provide a secure online credit card payment solution integrated into the University's finance system. This provides a secure environment for the capture of credit card details and the processing of payments directly into the University bank account.
- Students can pay fees with their credit card by logging into the student portal or by paying in person at any regional Cashier's office ("card present"). Card present payments are processed through the University's EFTPOS terminals.

## Policy:

- All University managers operating budget centres where credit card transactions are utilised for the purpose of receiving payment for goods and services, must comply with this policy. No alternative credit card facility is to be used.
- Budget centres running conferences or selling goods and services who wish to accept payment by credit card, must first apply to Massey University's Information Technology Services Department (ITS) by contacting servicedesk@massey.ac.nz in the first instance for access to the Credit Card Online Payment Facility. A "Store" ID must be issued by the Treasury team in Financial Operations.
- ITS is responsible for all network security and the provision of the University Online Payment Gateway.
- Online credit card refunds must only be processed by the Accounts Receivable or Treasury teams.
- The Treasury team must reconcile all online credit card payments to the University bank account and will audit / review any refunds that are processed through EFTPOS terminals.

*© This Policy is the property of Massey University*

- The Treasury team are responsible for the disposal of any miscellaneous manual credit card details received by email in accordance with the PCI DSS.
- Sensitive card information must not be held by Massey University but must be held on a secure server operated by the bank's solution provider.
- Credit/debit card details entered by Accounts Receivable or Te Paepoto on behalf of students, should only be keyed directly into the payment screen in the student portal, and must never be written down.

## Audience:

All staff.

## Relevant Legislation:

N/A

## Legal Compliance:

Payment Card Industry Data Security Standards (PCI DSS) requires merchants (i.e., Massey University) and service providers that store, process and transmit credit card information to comply with a set of security standards established to prevent loss, fraud and misuse,

## Related Procedures/Documents:

Credit Card Security and Compliance Procedures – Managing Income
Payment Card Industry Data Security Standard (PCI DSS)

## Document Management Control:

Prepared by: Chief Finance Officer

Authorised by: Deputy Vice-Chancellor – University Services

Date issued: August 2022

Last review: August 2022

Next review: August 2027

*© This Policy is the property of Massey University*