UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
PROCEDURE

Procedures:	**CASH CONTROL**
Parent Policy:	Cash Control Policy
Effective Date:	October 28, 2010
Revised Date:	July 1, 2013
Review Date:	October 28, 2020
Approving Body:	Administration: Vice-President (Administration)
Authority:	Policy: Cash Control
Responsible Executive Officer:	President, delegated to Vice-President (Administration)
Delegate:	Comptroller
Contact:	Comptroller
Application:	All Employees

Part I
Reason for Procedure

1.1 To establish procedures secondary to the Policy entitled "Cash Control" with regards to:

(a) the safekeeping of cash;

(b) cash receipting;

(c) debit and credit card payments;

(d) debit and credit card receipting;

(e) PCI-DSS compliance;

(f) payment card data storage guidelines.

Part II
Procedural Content

2.1 Cash is defined as all forms of payments received by the University including cash, cheques, money orders, bank drafts, wire transfers, but excluding debit

and credit card transactions. These are addressed separately in Sections 2.8-2.16.

2.2 All departments of the University receiving cash payments are responsible for its custody and safekeeping of the cash until deposited with Financial Services Cashiers' Office or directly with the University's bank.

2.3 The following procedures shall apply to all departments receiving payments:

(a) Cash must be safeguarded at all times in a locked safe or by other secure means.

(b) Cash must be deposited at the earliest practical opportunity, but in all cases by the next business day.

(c) Cash must be deposited into an authorized University bank account administered by Financial Services.

(d) Cash must be deposited in its entirety and under no circumstances may it be disbursed directly (e.g., to fund purchases, to cash personal cheques, or to replenish petty cash funds).

(e) Cash (bills and coins) must not be forwarded through internal mail due to the risk of loss or theft.

(f) Segregation of duties and restricted access to cash must be maintained at all times. At a minimum, segregation of duties shall include the separation of cash handling from the control and reconciliation of receipts.

(g) Remittances to the University in the form of cheques and bank drafts must be payable to "The University of Manitoba".

(h) Departments are responsible for providing the appropriate Fund/Organization/Account/Program (FOAP) coding for posting deposits to the general ledger.

(i) Departments must notify Revenue, Capital and General Accounting (RCGA) of the details of wire transfers into a University of Manitoba bank account in advance of the wire transfer.

(j) Departments that submit deposits directly to the bank must submit two copies of the Bank Transmittal Form, one to the bank and one to RCGA for subsequent verification of the deposit. This form is available on the Financial Services web site.

Cash Receipting

2.4 All cash receipts must be properly recorded and accounted for using a receipting system approved by Financial Services. Financial Services may authorize a department to maintain its own receipting system in situations where the unit processes a significant volume of transactions, and/or where the unit accepts payment cards (see 2.8-2.16 below for additional information).

2.5 Cash receipts must include specific information related to the transaction such as receipt date, customer name, amount, department, type of payment, and description of sale or service. For further information, contact RCGA.

Cash Receipts Issued by Financial Services:

Receipts Procedures

2.6 Departments that routinely process cash sales must manually record each transaction in a sales journal and issue a University authorized receipt to the purchaser. In receiving and recording payments departments shall:

(a) Obtain a receipt package consisting of pre-numbered receipts and "Cash Receipts and Distribution Journals" (also known as V-receipts) from the Cashiers' Office. The department must sign for the receipts and assign a contact individual to account for all receipts that have been signed out.

(b) Issue receipts for cash received. At the time of payment the customer shall be given the original copy of the receipt and a copy will be retained by the department.

(c) On a daily basis, the department shall complete and sign the Cash Receipts and Distribution Journal used that day, including the "Receipts Reconciliation" section at the bottom of the journal; and

(d) Deliver the journal and cash to the Cashiers' Office. The Cashier will issue an on-line receipt based on the FOAP(s) provided for the deposit. Cash shortages and overages must be identified and explained as part of the reconciliation.

Farm Sales Receipt Book Procedures

2.7 Department that process farm sales shall follow the following process:

(a) Obtain a Farm Sales receipt book from the Cashiers' Office.

(b) Issue the receipts for cash received. The department shall also provide a copy of each receipt to the Cashiers' Office and retain a copy for the departments' records.

(c) Reconcile the total and submit it to the Cashiers' Office along with a "Receipt Reconciliation Sheet", a copy of each receipt and the cash.

2.8 Cancelled or Void 'V' or Farm Sales receipts must be forwarded to the Cashiers' Office with the regular deposit.

2.9 Outstanding 'V' or Farm Sales receipts are subject to review by Financial Services after six months and must be returned to RCGA for reconciliation.

2.10 One-time payments such as cheques for contracts or grants shall be submitted directly to the Cashiers' Office along with a memo detailing the purpose of the payment, a department contact name and number, and the appropriate FOAP.

Debit and Credit Card Payments

2.11 VISA, MasterCard, and Interac debit (payment cards) are accepted methods of payment for University of Manitoba sales and services, with the exception of payment for degree related tuition revenue.

(a) Departments are required to use TC Merchant Services, the approved merchant services provider for the University of Manitoba, for all in-person (card present), card not present (e.g. telephone transactions), and electronic commerce activity.

(b) Departments wanting to accept payment cards for the first time (new merchants) must submit a written application form signed by the Business Manager for the faculty or administrative department to which the merchant reports.

(c) Information about becoming a payment card merchant or merchant services in general is available from RCGA:

http://umanitoba.ca/admin/financial_services/revcap/university_revenue.html

2.12 Departments offering the sale of goods and/or services through an authorized web site hosted on University of Manitoba servers must refer to Information Services and Technology ("IST") Technical and Functional guidelines for setting up their web application. Click here for details:

http://umanitoba.ca/computing/ist/internal/admin_sys/director/guidelines/index.html

Debit and Credit Card Receipt Procedures

2.13 Deposits for those departments utilizing debit/credit card merchant services are electronically transmitted to the bank. The process for recording deposits is as follows:

(a) RCGA is responsible for recording the deposit in the general ledger by journal entry, based on the daily deposit amount associated with each

merchant number on the bank statement, using accounting information provided by the merchant.

(b) For each receipt method, end of day batch totals provided by the option in place must be reconciled by the merchant to the deposit recorded in the general ledger by Financial Services.

(c) Any variance must be reported by RCGA and investigated by the merchant.

(d) Departments shall be advised by RCGA of chargebacks or deposit errors as soon as the information is made available by the bank.

2.14 Receipts must be issued to the customer, regardless of the processing option in place. Receipt content must meet the requirements specified by the TD Merchant Services Agreement and also be in compliance with Payment Card Industry Data Security Standards (PCI DSS) requirements.

Payment Card Industry Data Security Standards (PCI DSS) Compliance

2.15 The University of Manitoba must conform to Payment Card Industry Data Security Standards (PCI DSS) and Payment Application Data Security Standards (PA-DSS). The list of related requirements and guidelines is available at:

http://umanitoba.ca/admin/financial_services/revcap/university_revenue.html

(a) The main goal of PCI DSS is to protect confidential data at all points in the payment system. Merchants, payment application vendors, service providers, financial institutions, hardware (such as POS terminals and pinpads) and networks must protect cardholder information to prevent a breach of data security. It is the individual merchant's responsibility to ensure that procedures are in place to comply with PCI DSS requirements.

(i) Only individuals who need to access or use cardholder information should do so, accessing only the information needed to perform their job functions. Access of more than the minimum information needed by any University of Manitoba employee is prohibited.

(ii) University of Manitoba employees who have access to cardholder data are responsible to hold the data in confidence at all times. Cardholder information should be disclosed only for a required business purpose.

(iii) Departments that purchase standalone payment applications must receive written confirmation from the software vendor that the application complies with both the Payment Application Data Security Standards (PA-DSS) and the Payment Card Industry Data

Security Standards (PCI DSS) requirements. The application must also be configured to interface with University of Manitoba approved service providers, including TD Merchant Services and Beanstream.

2.16 All University of Manitoba merchants are required to confirm their compliance with PCI DSS requirements on an annual basis by completing and submitting an "Attestation of Compliance" form to RCGA. New merchants will be required to confirm that PCI compliant procedures are in place prior to activating a new merchant account. Merchants that are found to be non-compliant will be subject to cancellation of their merchant status if the situation cannot be remedied within a reasonable amount of time.

2.17 If credit card information has been compromised or improperly accessed or used, or if any systems or security measures protecting cardholder information have been breached, the merchant must immediately report the breach to the Comptroller.

2.18 Merchants must comply with the University's electronic data storage policy. This Policy is administered by IST and may be found on IST's website.

Recommended Payment Card Data Storage Guidelines

2.19 Guidelines for meeting PCI DSS compliance requirements are summarized as follows:

(a) Merchants may store only the Personal Account Number, expiration date, service code, and cardholder name, using precautions for safe storage.

(b) Where applicable, merchants must encrypt printed personal account numbers to ensure that all but the last 14 digits are suppressed or masked when displayed or printed on receipts or retained in files.

(c) Paper media containing cardholder data must be securely stored in a locked environment for a 12-month retention period (VISA) or 18-month retention period (Master Card) that corresponds with the allowed chargeback period per the University of Manitoba's Merchant Services agreements. Failure to provide a copy of a receipt when requested could result in a chargeback.

(d) Merchants must assign responsibility for ensuring that storage standards are maintained and strict control is maintained over access to the stored documents.

(e) Merchants must shred or destroy documents after 12 (VISA) or 18 (Master Card) months in a manner that prevents reconstruction of the information, once the receipt information is no longer required for business purposes.

(f) Merchants must not disclose data except for business purposes.

(g) Merchants must never send or receive credit card information by e-mail. If an e-mail that includes credit card information is received, the e-mail must be deleted from both the inbox and deleted items folder. Trash must be purged/expunged. Remove all cardholder information before replying.

(h) University of Manitoba employees with access to cardholder data are responsible for holding the data securely and confidentially at all times.

(i) Merchants must never leave credit card information unattended.

Part III
Accountability

3.1 The Office of Legal Counsel is responsible for advising the Vice President (Administration) that a formal review of this Procedure is required.

3.2 The Comptroller is responsible for the interpretation, administration and review of this Procedure.

3.3 All employees are responsible for complying with this Procedure.

Part IV
Review

4.1 Governing Document reviews shall be conducted every ten (10) years. The next scheduled review date for this Procedure is October 28, 2020.

4.2 In the interim, this Procedure may be revised or repealed if:

(a) the Vice President (Administration) or Approving Body deems it necessary or desirable to do so;

(b) the Procedure is no longer legislatively or statutorily compliant; and/or

(c) the Procedure is now in conflict with another Governing Document.

(d) the Parent Policy is revised or repealed.

Part V
Effect on Previous Statements

5.1 This Procedure supersedes all of the following:

(a) all previous Faculty/School Council Procedures stemming from the Faculty/School Council Bylaw and academic and admission Regulations and any resolutions on the subject matter contained herein;

(b) Policy 306 “University Receipts”;

(c) Procedure “Cash Control” effective August 12, 2008;

(d) all previous Board of Governors/Senate Governing Documents on the subject matter contained herein; and

(e) all previous Administration Governing Documents on the subject matter contained herein.

Part VI
Cross References

6.1 This Procedure should be cross referenced to the following relevant Governing Documents, legislation and/or forms:

(a) Cash Control Policy