POLICY

Policy Title:	Cash and Credit Payments	Last Revision:	
Policy No:	3002	Approval Date:	August 08, 2019
Approval Body:	President's Office		
Policy Date:	September 01, 2019	Review Date:	August 12, 2019

Purpose

UCW Finance department is the only team which can handle cash/equivalents and it's important that appropriate procedures are in place to prevent loss, promote security and ensure accurate financial reporting.

Procedure:

To minimize the potential for mistakes or misappropriation of cash, the segregation of cash handling duties is required. The duties of collecting cash, maintaining documentation, preparing deposits, and reconciling records is distributed between two or more individuals. At a minimum, deposits must be reviewed and signed off on by someone who did not prepare the deposit, prior to submitting it for processing.

For non-recurring transactions, such as store sales, payments for students' trips etc, unless under extenuating circumstances, the cash or equivalents and receipts must be handed over to UCW Finance department on the same day as the transaction occurs.

UCW encourages the students to cover tuition costs via wire transfer, using secure payment portal www.paymytuition.com or cheque payment.

UCW can only accepts up to max of $300 in cash per student per day.

- **Employee Training and Background Checks:**

When hiring part-time or full-time employees who handle cash receipts as part of their duties within Finance department, references should always be requested and verified.

Staff engaged in receipts processing should have mandatory training including a thorough review of the department's written procedures. Head of the department is responsible to provide periodic refresher training, at least on an annual basis, to ensure employees are in compliance with these procedures.

- **Physical security/safeguarding assets and information**

Finance staff handling cash receipts are responsible for the safekeeping of these University assets.

The following measures promote a safe work environment and ensure the secure handling of cash receipts:

- Restrict access to cash to as few people as possible.

- Cash drawers should be closed when not in use and locked when not attended.
- Store cash or personal information in a locked, non-portable cabinet. Provide combinations and passwords only to authorized personnel.
- Change combinations and passwords annually and with any turnover of related personnel.
- Perform balancing and prepare deposits in a non-public, secure area that is not easily visible to others.
- Provide deposits finance daily
- Pending deposit, cash and equivalents must be held in a secure location such as a locked cash box in a locked filing cabinet, a lockable cash drawer, or a safe.
- The degree of security required will depend on the amount of the currency normally handled and the environment. When the daily balance of cash on hand averages more than $1,000, it must be locked in a combination safe.
- Where credit card payments are accepted, storage and access must follow the minimum Payment Card Industry (PCI) requirements. Inspect POS machines daily for tampering and substitution. Only use POS terminals in an area where access is restricted to those who have received PCI Compliance training.
- Business Operations maintains a list of POS terminals. Merchant units must immediately notify the Supervisor-Cash Receipts when a POS terminal is replaced or a new terminal is added or removed from the unit.
- Each business units is responsible for safeguarding the confidentiality of sensitive data relating to the sale or purchase of goods and services. Information gathered about customers must be maintained in a secure manner, restricted to individuals who have a need to know and must only be used for the purpose for which it was provided.
- Business units must comply with information privacy legislation and with University policies on information privacy.

- **Prompt Deposit of Cash Receipts**

Cash receipts totalling $1,500 or more must be deposited no later than the next business day. Receipts totalling less than $500 must be deposited within 5 business days.

If no physical cash or cheques are included in the deposit, the reconciliation/deposit must be provided to Receipt Accounting within 5 days of the transaction processing date.

Revenue will not be credited to departmental accounts until a reconciliation of the amounts are received and accepted.

- **Reconciliation of Cash Receipts**

To ensure that all sales are recorded, a daily routine for balancing cash receipts must be followed, including processes for balancing cash, cheques, credit and debit cards.

Balance all cash collected daily by comparing the total cash to the cash register or cash receipt journal/log. All credit card sales should be compared to the Daily Settlement reports provided by the POS terminals or the electronic database/reporting tool.

Compare the departmental copy of the deposit receipt with the revenue recorded in Finance system weekly. Report all unreconciled items to Receipt Accounting on a weekly basis.

- **Receipting**

Receipts should be provided to the customer for any sale of a good or service

- **Post-dated Cheques**

Only cheques that are dated on or earlier than the current date can be included in the department's deposit. Those employees involved in deposit preparation must ensure that the date found at the top-right corner of the cheque is verified as current or prior to the current date.

- **Dishonoured or Returned Cheques**

Most dishonoured cheques occur because the maker of the cheque has either stopped payment or does not have sufficient funds in their account. Finance will notify the department via email of the returned cheque. Any returned cheque will be debited to the revenue account originally charged.

Since a dishonoured cheque represents a debt to the University, the matter must be addressed promptly with the maker of the cheque. Departments are responsible for immediate follow-up of any returned items and subsequent prompt depositing of the replacement funds.

Note that bank regulations preclude the re-depositing of any returned item, and therefore cash, a certified cheque, or money order should be obtained in its place.

Incoming Wire Payments Customers making payments from outside of Canada should be encouraged send their payment via wire into UCW bank account unless it is a tuition payment, whereas they should follow the instructions on the UCW website. Wire payments are convenient for both parties, and provide enhanced security while at the same time reducing the time involved in the clearing process. Wire payments are more efficient than cheques or money orders.

- **Report all Breaches**

Suspected or confirmed theft of cash receipts, inventory or other University assets should be reported immediately to the office of the Campus Security and Finance department.

Suspected credit card breach should be reported immediately following the process outlined in the Cardholder Data Security Incident Response Plan.

Requirements for Credit/Debit Card Processing:

There are additional considerations should a department/unit wish to accept debit or credit cards (including e-commerce) for payment. The general guidelines to be a credit/debit card merchant are as follows:

- Head of Finance team is responsible for training annually staff who has access or can impact the Cardholder Data Environment: This may include technical staff members in the unit. Should third party software be used in the payment process (including recording, storage and/or transmission of credit card data), the merchant department is responsible for obtaining the appropriate documentation to support the third party provider's PCI compliance
- If credit card data is taken over the phone, it must be keyed directly into a Point of Sale (POS) terminal and not stored. The phone line must have the voice mail option disabled.
- If Point of Sale terminals are used, they must be regularly inspected for tampering
- All staff must have a unique password for the payment environment – generic passwords such as "morning shift" are not allowed.
- All individuals must be aware of and understand the Incident Security Response protocol in the event of a breach or suspected breach of data or equipment.
- The university has one vendor of choice for processing credit card transactions. All payment applications will use this vendor for financial transaction processing. If the vendor of choice is unable to provide the required service, a business case must be made to support moving to a different vendor and the regular approval process
- All debit/credit transactions must be processed in Canadian dollars.
- The merchant department is responsible for all charges and fees related to credit/debit card processing. Costs include initial setup, monthly support fee, per transaction fee and merchant discount. All fees and charges are subject to change.
- Departments using e-commerce/payment websites are required to reconcile their daily sales transactions to the merchant reporting tool on a daily basis.
- Any changes to a live payment processing environment must be reapproved prior to the changes being placed in production, including if necessary, updated third party vendor PCI compliance documentation.
- Merchants must treat cardholder data as "Sensitive" or "Confidential" as outlined in UCW's Data and Information Classification and Protection Policy.