

# Cash/Equivalent Receipt Handling Procedures

---

## Purpose

Departments handling cash/equivalents must have the appropriate procedures in place to prevent loss, promote security and ensure accurate financial reporting.

## Table of Contents:

1. Written Procedures
2. Segregation of Duties
3. Employee Training and Background Checks
4. Physical security/safeguarding assets and information
5. Prompt Deposit of Cash Receipts
6. Cash receipts must be deposited intact
7. Collecting and Remitting Taxes
8. Completing Deposit Forms
9. Reconciliation of Cash Receipts
10. Receipting
11. Post-dated cheques
12. Dishonoured or Returned Cheques
13. Receipt of Payment for (GAR) Invoicing
14. Incoming Wire Payments
15. Deposit Errors
16. Report all Breaches
17. Additional Requirements for Credit/Debit Card Processing
18. Template for Departmental Cash Handling Procedures

The following are addressed in the procedural documents and must be adhered to;

### 1. Written Procedures

Each department that handles cash and cash equivalents must have its own written procedures tailored to its specific operation. The departmental procedures should include, but are not limited to the following:

- List of anticipated payment types (e.g. cash, cheques, e-commerce) and appropriate processing and internal controls for each. A description of how payments are received (e.g. in person, by mail, online) and the methods for ensuring secure storage before, during and after processing.

- A documented receipting process, including a sample receipt and forms control mechanism (e.g. sequential numbering). Canada Revenue Agency guidelines must be followed regarding the reporting of HST if receipt is for the sale of a taxable good or service.
- Identification of positions assigned to each step in the procedure(s), ensuring proper segregation of duties.
- A description of how deposits are made, including the method and frequency.
- A description of the process to reconcile deposit activity to a unit's revenue.
- A description of the unit's return/refund process.

Departmental procedures should be initially approved and subsequently reviewed annually by the Departmental Manager to ensure compliance with the University's Cash/Cash Equivalents Handling policy as well as other related policies and procedures.

For assistance in developing departmental procedures contact the Supervisor, Cash Receipt Accounting-Business Operations.

## **2. Segregation of Duties**

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 should be 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.

Refunds should be reviewed and approved by a Supervisor. Appropriate documentation supporting the refund should be retained.

In departments where the segregation of duties is not feasible, alternative and compensating controls may be implemented to achieve the desired objectives. Please contact the Assistant Manager – Business Operations for information on how to establish appropriate controls for your area. Establishing clear accountability for the handling of cash ensures that receipts are properly accounted for, revenue is secured, and revenue is traceable to specific handlers.

## **3. Employee Training and Background Checks**

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

Departments engaging in receipts processing should conduct mandatory training for all employees involved, including a thorough review of the department's written procedures. Departments are encouraged to provide periodic refresher training, at least on an annual basis, to ensure employees are in compliance with these procedures.

Mandatory PCI training is required for any individuals involved in the handling of Cardholder Data (credit cards). This training must be completed annually.

#### **4. Physical security/safeguarding assets and information**

Departments handling cash receipts are responsible for the safekeeping of these University assets. This includes both monetary assets as well as payment processing equipment. Department managers should review the cash receipt process and physical security should be emphasized to every employee involved in the process. 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 to Receipt Accounting, Business Operations daily
- Where there are items for sale, proper inventory control over these items should be established. The amount of inventory on hand should be counted on a regular basis and agreed to sales and inventory records.

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 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.

Where a credit card payment device is removed from Carleton University campus, the individual must ensure that the various components (including the phone/tablet, dongle, 'square', etc) are securely stored and safeguarded at all times. Additionally, they must employ multi-factor authentication (e.g. a password, plus a second authentication).

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.

Units are 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.

Units must comply with information privacy legislation and with University policies on information privacy.

#### **5. Prompt Deposit of Cash Receipts**

Due to University Insurance requirements, cash receipts totaling \$200 or more must be deposited no later than the next business day. Receipts totaling less than \$200 must be deposited within 5 business days.

Any single item equal to or exceeding \$100,000.00 should be immediately hand delivered to the

Business Office for immediate bank deposit.

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. Templates are available at <http://carleton.ca/financialservices/forms/>

## **6. Cash receipts must be deposited intact**

Reimbursements may not be provided from the department's cash receipts. Each deposit must correspond to the sales recorded for the period. If required, a petty cash fund should be used to reimburse minor expenditures and can be arranged through the Supervisor – Receipt Accounting.

## **7. Collecting and Remitting Taxes**

The university is considered a Public Service Body and a charity for tax purposes, which means typically we are not required to charge HST on services provided, but must charge tax on any goods sold to third parties (this includes external groups using Carleton facilities, such as student and employee unions, the Charlatan, etc).

HST is applied based on where the good/service will be consumed (used). In Ontario, the HST rate is 13%. However, this rate can vary from province to province. Please check [Sales to Third Parties Outside of Ontario](#) on the Financial Services tax website for applicable provincial rates.

HST is usually applied in addition to the list price of the good. It must be clearly shown separately on the deposit form and is to be deposited against the HST Payable account – 100000 225008.

Should the list price include HST, the tax amount must still be clearly separated on the deposit form and only the net (after tax) amount should be credited to the department's revenue account.

Each month Business Operations will remit the total taxes payable to Canada Revenue Agency on behalf of the university. If a deposit reconciliation has not been submitted by the tax remit deadline for the university, 13% of the gross amount may be deemed as tax payable and departmental revenue reduced accordingly. If a reconciliation is outstanding after two tax reporting periods, the unit will be asked to terminate their sales operations until it can reconcile all amounts outstanding and provide Financial Services with reassurance that it has the resources and expertise to manage the sales function.

## **8. Completing Deposit Forms**

Appropriate sales taxes must be recorded and reported as part of the deposit to allow the Business Office to prepare remittances to the proper tax authorities.

Source documents, such as cash register tapes, credit and debit card receipts should be forwarded to Receipt Accounting to support the deposit. Source documents supporting the unit's order/sale transactions should be retained by the unit/department for seven years as per Canada Revenue Agency guidelines.

Deposit forms must be prepared for each day's activity and must accompany the deposit to Receipt Accounting. Separate deposit forms must be prepared for **each** currency. The table below describes which form to use and the delivery method required.

Currency	Carleton University Form(s)	Where to Deposit
Canadian	Canadian deposit form (cash/cheque)  Canadian deposit form (cash/cheque/credit and debit)  Canadian deposit form(credit and debit)	1. Delivery in person to Receipt Accounting , Business Office, 301 Robertson Hall, <b>or</b> 2. Pick-up via Brink's secure transportation, where volumes are warranted and service has been arranged through Receipt Accounting.  3. E-Commerce deposit reports may be emailed to <a href="mailto:receipt.accounting@carleton.ca">receipt.accounting@carleton.ca</a> .
USD	US Funds deposit form	1. Delivery in person to Receipt Accounting, Business Office, 301 Robertson Hall, <b>or</b> 2. Pick-up via Brink's secure transportation, where volumes are warranted and service has been arranged through Receipt Accounting
Other currencies	Foreign Funds deposit form	Send to Receipt Accounting who will make the deposit with the bank.

It is preferable that all deposits remitted to Receipt Accounting are delivered in person. However any deposits containing cash or travelers cheques **must** be delivered to Receipt Accounting, 301 Robertson Hall **in person**, without exception.

### *Completing a Canadian Deposit Form*

- Download the Canadian Deposit Form found at <http://www.carleton.ca/financialservices/forms/>.

The form has been designed to be completed online, but may be completed by hand if necessary. The online version provides two major benefits:

- an automated tracking number used to track the deposit throughout its lifecycle
  - advanced formulas that calculate totals and validate the input of key fields.
- The 'Total Receipts' located in the 'Canadian Funds Deposit Memo' must equal the 'Total Distribution' in the Revenue Distribution Section.
  - Indicate the date the form was prepared.
  - Indicate who prepared the deposit as well as who reviewed the deposit (a supervisor).
  - A mandatory field on the form is the 'description of the Product or Services sold'. This notation provides information on how Harmonized Sales Tax (HST) may apply to the sale of good or service.
  - Remit the funds, supporting documentation and deposit form to Receipt Accounting.

### ***Completing a USD Funds Deposit Form***

*Note: A separate form must be prepared for each type of currency being deposited.*

1. Download the USD Deposit form at <http://www.carleton.ca/financialservices/forms/>  
The form has been designed to be completed online, but may be completed by hand if necessary.

The online version provides two major benefits:

- an automated tracking number used to track the deposit throughout its lifecycle
  - advanced formulas that calculate totals and validate the input of key fields.
2. The 'Total Receipts' located in the 'US Deposit Memo' must equal the 'Total Distribution' in the Revenue Distribution Section.
  3. The form must indicate the date it was prepared.
  4. The form must indicate who prepared the deposit as well as who reviewed the deposit (a supervisor).
  5. A mandatory field on the form is the 'description of the Product or Services sold'. This notation provides information on how Harmonized Sales Tax (HST) may apply to the sale of good or service.
  6. Remit the funds, supporting documentation and deposit form to Receipt Accounting. Once the deposit has been made to the bank and the foreign exchange amount known, Receipt Accounting will credit the departmental revenue accordingly.

### ***Completing a Foreign Funds Deposit Form***

*Note: A separate form must be prepared for each type of currency being deposited.*

1. Download the Foreign Funds Deposit form at <http://www.carleton.ca/financialservices/forms/>  
The form has been designed to be completed online, but may be completed by hand if necessary.
2. The 'Total Receipts' located in the 'Foreign Deposit Memo' must equal the 'Total Distribution' in the Revenue Distribution Section. Note: The currency must be identified at the top of the form and each denomination of cash included in the deposit must also be indicated.
3. The form must indicate the date it was prepared.
4. The form must indicate who prepared the deposit as well as who reviewed the deposit (a supervisor).
5. A mandatory field on the form is the 'description of the Product or Services sold'. This notation provides information on how Harmonized Sales Tax (HST) may apply to the sale of good or service.

6. Remit the funds, supporting documentation and deposit form to Receipt Accounting. Once the deposit has been made to the bank and the foreign exchange amount known, Receipt Accounting will credit the departmental revenue accordingly.

## **9. 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, Campus Cards, 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 FAST Finance monthly, at a minimum. Report all unreconciled items to Receipt Accounting on a monthly basis.

## **10. Receipting**

Receipts should be provided to the customer for any sale of a good or service and should either originate from a cash register or a pre-numbered register, if hand-written. They should include the date, a description of the sale, the amount and tax information, if required.

If the sale is taxable, the university's HST registration number must be included on the receipt. Additionally, the receipt must indicate that tax was included in the total sale, by either:

- Breaking out the amount of GST/HST paid on the supply, or
- Indicating that the price of the supply includes GST/HST

You may indicate the tax amount by showing the dollar value of the tax or the rate at which the tax was applied.

## **11. 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 post-dated items that are inadvertently processed in advance of the cheque date will be stamped 'Item Dishonoured' and an image of the cheque will be returned to the department.

Any dishonoured post-dated item cannot be certified and then re-cleared. If this situation arises, the depositing unit will need to make arrangements directly with the cheque maker to obtain a replacement cheque and then re-deposit that replacement cheque.

## **12. 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. Receipt Accounting 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.

### **13. Receipt of Payment for (GAR) Invoicing**

When a request is made to Business Operations to invoice an external client, the revenue is credited to the department's revenue account at the time the invoice is generated.

If a payment is received by the department for an invoiced amount, forward it for deposit to Receipt Accounting, Business Operations, 301 Robertson Hall to credit the amount owed to the university. Include the invoice number, if available.

### **14. Incoming Wire Payments**

Departments who regularly receive payments from outside of Canada should encourage their customers to send their payment via wire into Carleton's bank account. 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.

Instructions for completing an incoming wire payment may be requested from Receipt Accounting – [receipt.accounting@carleton.ca](mailto:receipt.accounting@carleton.ca).

### **15. Deposit Errors**

In the unlikely event that the Bank of Nova Scotia discovers an error in a deposit, the amount will either be debited or credited to the 716702 over/short account. Departments will be advised of the error via email and will be responsible for reconciling and adjusting their accounts.

### **16. Report all Breaches**

Suspected or confirmed theft of cash receipts, inventory or other University assets should be reported immediately to Campus Security and to Receipt Accounting, Business Operations.

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

### **17. 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:

- Merchant units must be familiar with and adhere to the PCI compliance requirements, including:
  - All staff who have access to or can impact the Cardholder Data Environment must attend annual mandatory training. 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. This includes, but is not limited to, an Attestation of Compliance, typically in the form of an SAQ D – SP (Self-Assessment Questionnaire “D” for Service Providers), which must be updated annually or if the software changes – e.g. updates
  - Merchants will not collect or store any credit/debit card data in any form (electronic or paper). Where the PAN or Primary Account Number of the credit card is presented (e.g. on a receipt), the numbers must be masked with only the last four numbers legible.
  - Merchants will not accept credit card data via email. 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. Evidence of the inspections (e.g. inspection logs) are to be submitted to the PCI Compliance Officer - Financial Services quarterly – by the end of July, October, January and April of each fiscal year.
  - All staff must have a unique password for the payment environment – generic passwords such as “morning shift” are not allowed.
  - System “owners” (unit managers) must have documented procedures for access control and must be able to produce the documented procedures, when required, for auditing purposes. Evidence of account approval, termination and disabling must be available when required for auditing purposes.
  - 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 (as described below) must be met.
- All payment websites will adhere to Carleton University's protection of privacy policies.
- 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 Carleton’s Data and Information Classification and Protection Policy.

**Requesting/Establishing a merchant:**

Any department/unit interested in accepting payment via credit/debit card must first contact the [Assistant Manager, Business Operations](#) for an initial consultation. If a decision is made to proceed, the appropriate merchant type will be determined (e.g. e-commerce, Point of Sale machine).

#### 1. Website/E-commerce

Website development must be done in consultation with the IT Security, ITS and the Assistant Manager, Business Operations in order to ensure effective mitigation of information technology risk and to ensure PCI Compliance. Once the website development is complete, Business Operations and IT Security will make a recommendation to the AVP- Financial Services regarding final approval of the website prior to go-live.

- Business Operations will make their recommendation based on adherence to the Cash Handling policy, as evidenced by the details included on the internet transaction receipt described below as well as a demonstrated internal controls and the ability to reconcile and report on transactions.
- IT Security will provide approval and make their recommendation after it has been demonstrated that the website has sufficiently mitigated the IT risk to an acceptable level. Included in the assessment, IT Security will evaluate the Operational Risk, reviewing such issues as setting of security flags and access to site.

Final approval of the web-site must be provided by the AVP – Financial Services.

A copy of the internet transaction receipt(s) must be included as supporting documentation for final approval. It should include at a minimum:

- The date that you obtained the processing data for the relevant Internet Transaction;
- Your Merchant number applicable to the Internet Transaction(s);
- Your business trade name and Web Site address;
- The Card type used in the Internet Transaction - DO NOT INCLUDE THE CREDIT CARD NUMBER;
- The amount and type (purchase or credit) of the applicable Internet Transaction;
- The currency in which the Transaction was processed (CDN);
- The authorization number assigned to the Internet Transaction;
- The unique Internet Transaction order number assigned by you;
- A detailed description of the Internet Transaction goods or services;
- The contact name, mailing address, electronic mail address, telephone and fax number of person representing you for Internet Transaction disputes;
- Applicable Merchant taxation or export information;
- The name of the purchaser of your goods or services;
- Return/refund policy

#### 2. Point of Sale Machine

Rental of a Point of Sale machine is arranged through the Cash Office, Business Operations. Prior to installation of the machine, the merchant department must request, via the ITS Service Desk, the installation of a dedicated VoIP jack installed specifically for the POS machine. This restricts transmission of credit card data to a segmented and secure local area network.

## **18. Template for Departmental Procedural Manual**

Each department or unit involved in collecting revenue on behalf of the university must have a documented process for handling the cash and cash equivalents received on deposit.

This provides a standardized, auditable methodology for your department and can be used as a training tool for new employees. The use of a standard process reduces the risk to the individual employees, the department and the university.

Should you have any questions or require assistance to complete your departmental process guide, please contact the Cash Office Supervisor, Financial Services.