

## **POLICY 1.29 – Bank Card Policy**

**Policy Category:** General

**Effective Date:** June 26, 2007

**Supersedes:** June 28, 2001

---

### **PURPOSE**

The acceptance of Bank Cards provides a convenient way to handle the sale of goods and services at The University of Western Ontario. While University departments are encouraged to use technology, there is a need to understand the information security risks associated with the transaction. In particular, electronic commerce transactions introduce a high level of risk with respect to the security and privacy of the personal information of purchasers. Departments must meet the University's requirements for security and for integrating transaction information into the University's application systems.

By permitting the use of Bank Cards for commercial transactions, The University of Western Ontario becomes subject not only to federal and provincial legislation relating to privacy, but also rules and regulations relating to the handling of Bank Cards and Cardholder Information imposed by Banks and other third parties. This Policy provides mandatory security measures and procedures for University departments accepting Bank Cards for payment.

### **DEFINITION**

Bank Card

Bank Card means credit cards, debit cards, ATM cards, and any other card or device, other than cash or cheques, issued by a bank or credit union, which is normally presented by a person for the purpose of making a payment.

PCI Standards

The Payment Card Industry (PCI) Data Security Standard was created by major credit card companies to safeguard customer information. Visa, MasterCard, American Express, and other credit card associations mandate that merchants and service providers meet certain minimum standards of security when they store, process and transmit cardholder data.

### **POLICY**

- 1.00 The Bank Card Committee advises and makes recommendations on all matters associated with transactions involving Bank Cards, including electronic commerce activity, at the University.

## POLICY 1.29 – Bank Card Policy

- 1.01 Membership of the Bank Card Committee is:
- Associate Vice-President (Finance & Facilities) - Chair
  - Information Technology Services – Client Support Associate Director, Information Security Officer
  - Financial Services – Supervisor, General Accounting
  - Internal Audit – Director, Internal Audit
  - Western Information Systems Group – Corporate Data Security Officer
  - Three members from departments that accept Bank Card payments appointed by the Chair, for individual terms of up to 3 years, renewable
- 2.00 The *Bank Card Procedures* developed and approved by the Bank Card Committee govern the approval, installation, operation and management of Bank Card activity at the University. It shall be the responsibility of all members of the University community to comply with the Bank Card Procedures.
- 3.00 The *Bank Card Procedures* shall be reviewed on an annual basis by the Bank Card Committee in order to accommodate developments in the interpretation of the PCI Standards, legislation, developments in the technology involved in Bank Cards, and developments in the use of such technologies, and to ensure that it complies with all applicable laws and University policies, including laws and policies relating to privacy and access to information.
- 4.00 The development of web sites which propose the electronic payment of goods and services must be reviewed with the Bank Card Committee and approved by the Vice-President (Operations & Finance).
- 5.00 Departments that provide electronic commerce sites may be subject to an external security audit, at the expense of the department, prior to the implementation of the electronic commerce site and/or in accordance with the *Bank Card Procedures*.
- 6.00 An agreement to securely accept credit card payments has been negotiated between the University, an authorized electronic commerce provider and a financial institution. Departments must not enter into separate banking arrangements.
- 7.00 Departments are responsible for safeguarding the confidentiality of sensitive data and personal information relating to the sale or purchase of goods and services and for ensuring compliance with information privacy legislation and with University policies on information privacy. Safeguards include, but are not limited to the following:
- 7.01 Electronic commerce sites must have mechanisms to ensure information collected, transmitted and stored electronically is protected from unauthorized access and that access is restricted to individuals who have a valid reason to know.
- 7.02 Customers must be informed of the purpose(s) to which the information will be put and personal information gathered about customers must only be used for those stated collection purposes.
- 7.03 Information collected about purchasers must be maintained in a secure manner and disposed of in a secure manner once no longer needed for the purpose(s) for which it was collected.
- 8.00 Information gathered about customers must only be used for the purpose for which the information was given.

**SECURITY INCIDENTS**

Any release or exposure of Cardholder Information to an unauthorized third party, or unauthorized access to a Bank Card System must be reported to a member of the Bank Card Committee and Legal Counsel. An emergency response plan will be implemented as necessary.

**ENFORCEMENT**

Ecommerce servers not in compliance with this policy may be removed from service. Departments involved with non-compliant ecommerce sites may be precluded from taking part in further commercial activity involving the use of Bank Cards.

**REVIEW AND UPDATE PROCESS**

- 1.00 The Associate Vice-President Financial Services shall, in consultation with the Bank Card Committee, review this Bank Card Policy no less frequently than every three years.
- 2.00 The Bank Card Committee shall review the *Bank Card Procedures* and the PCI Data Standards annually to ensure they result in effective and efficient protection against current risks.
- 3.00 A review shall be conducted if a significant loss occurs due to a risk that has not been adequately addressed in either Policy or Standards.