|  |  |
| --- | --- |
|  | THE UNIVERSITY OF BRITISH COLUMBIA (CBM, *Academic Systems, UBCIT*) |

|  |  |
| --- | --- |
| **Requirement 6: Develop and maintain secure systems and applications** | |
| **6.6 Are all web-facing applications protected against known attacks by applying either of the following methods?**  **1. Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security.**  **2. Installing an application layer firewall in front of webfacing applications.** | |
| **Date of Issue:**  *August 1,2010* |

**PURPOSE**

The purpose of this document is to specify procedures for PCI Compliance requirement 6.

**POLICY**

These procedures relate to university policy 106 (Access to and Security of Administrative Information), and section 5 (PCI-DSS Requirements) of UBC’s Information Security Manual.

**PERSONNEL INVOLVED**

Senior Systems Analyst

Systems Analyst

Business Analyst

QA Lead

Software Architect

Project Manager

Academic Systems Support

Desktop services

Business Manager

**CONTACT INFORMATION**

For procedure enquiries, please contact:

Sharon Rashtian, Manager Academic Systems Support

Phone: 604-822-8886

Sharon.rashtian@ubc.ca

**PROCEDURE**

1. Administrators who have access to CBM’s Virtual Terminal for handling individual payments are equipped with a full suite of software from SOPHOS to handle Firewall as well as virus scan.
2. Trustwave monitors our admin and payment gateway server to ensure it has the proper level of security that is required for application. Academic Systems receives regular reports and if there are vulnerabilities or exploits in the system, it has been clearly identified in the report.
3. Code review by peers reduces the possibility of vulnerabilities in the system, and best practices in coding standards are being used by the development team.
4. Design review and approval by Software Architect ensures security of the system is also in place to ensure no new security risks are being introduced to CBM.

**REVISION HISTORY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Details of Change** | **Changed By** | **Approved By** | **Title** |
| (*Insert Date*) | (*Initial Version*) | (*Name*) | (*Name*) | (*Approver’s Job Title*) |