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

|  |  |
| --- | --- |
| **Requirement 6: Develop and maintain secure systems and applications** | |
| **Question**  **6.5a Are all web applications developed based on secure**  **coding guidelines such as the Open Web Application**  **Security Project guidelines?**  **6.5b Is custom application code reviewed to identify coding vulnerabilities?**  **6.5c Is prevention of common coding vulnerabilities covered in software development processes, including the following?**  **6.5.1 Unvalidated input?**  **6.5.2 Broken access control (for example, malicious use of**  **user IDs)?**  **6.5.3 Broken authentication and session management (use of**  **account credentials and session cookies)?**  **6.5.4 Cross-site scripting (XSS) attacks?**  **6.5.5 Buffer overflows?**  **6.5.6 Injection flaws (for example, structured query language**  **(SQL) injection)?**  **6.5.7 Improper error handling?**  **6.5.8 Insecure storage?**  **6.5.9 Denial of service?**  **6.5.10 Insecure configuration management?** | |
| **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

**CONTACT INFORMATION**

For procedure enquiries, please contact:

Sharon Rashtian, Manager Academic Systems Support

Phone: 604-822-8886

Sharon.rashtian@ubc.ca

**PROCEDURE**

1. As part of UBC’s payment gateway (CBM) architecture, separation of duties has been built into the system. The payment processing engine is deployed separately from the administration module which allows refunds and some reporting.
2. Access to the Administrative module for CBM has been managed by Academic Systems and SIS Security through special registration and account setup procedure.
3. Access levels are role based and users only gain access to the functionalities that are required for them to run their business.
4. CBM does not transmit or store any credit card information.
5. Trustwave monitors our admin and payment gateway server to ensure it has the proper level of security that is required for application. Especially Systems will be notified if there are risks with regards to XSS, Buffer overflows, and SQL injection into CBM.
6. 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.
7. Design review and approval by Software Architect ensures security of the system.

**REVISION HISTORY**

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