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

|  |  |
| --- | --- |
| **Requirement 6: Develop and maintain secure systems and applications** | |
| **Question**  **6.3a Are software applications developed based on industry**  **best practices, and do they incorporate information**  **security throughout the software development life cycle?**  **6.3b Do software development controls ensure the following?**  **6.3.1 Testing of all security patches and system and software**  **configuration changes before deployment?**  **6.3.2 Separate development, test, and production**  **environments?**  **6.3.3 Separation of duties between development, test, and**  **production environments?**  **6.3.4 Production data (live PANs) are not used for testing or**  **development?**  **6.3.5 Removal of test data and accounts before production**  **systems become active?**  **6.3.6 Removal of custom application accounts, usernames,**  **and passwords before applications become active or**  **are released to customers?**  **6.3.7 Review of custom code prior to release to production**  **or customers in order to identify any potential coding**  **vulnerability?** | |
| **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**

Academic Systems Support

Senior programmer analysts

Project manager

Systems analysts

Senior Systems analyst

Business Analyst

QA Lead

Software Architect

DBA

**CONTACT INFORMATION**

For procedure enquiries, please contact :

Sharon Rashtian, Manager Academic Systems Support

Phone: 604-822-8886

Sharon.rashtian@ubc.ca

**PROCEDURE**

1. UBC’s payment gateway (CBM) is built upon Java technologies. Java is the language of choice in financial industry across the globe. The structure of the language and the framework, avoids many vulnerabilities, therefore reduces the security risk at the application level.
2. The code is maintained in Fish-eye for code review, prior to the release.
3. Development, Test and Production environment are all separated at the application and database level.
4. All changes to the application are first developed in development environment (Sandbox and Integrate regions) then it moves to Test and finally after release gate review, it gets released to the production.
5. Changes and features go through rigorous QA testing to ensure bugs are not being introduced to the Production environment.
6. Production data has been altered prior to being moved to Test and development databases, therefore live PAN is never being used for testing.
7. UBC’s payment gateway does not store credit card information in any of the database instances.
8. Feature releases are reviewed by members defined in Systems software delivery process and it goes through SIS release gate review.

**REVISION HISTORY**

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