|  |  |
| --- | --- |
|  | THE UNIVERSITY OF BRITISH COLUMBIA (*MONERIS*) |

|  |  |
| --- | --- |
| **Requirement 4: Encrypt transmission of cardholder data across open, public networks** | |
| **Question 4.2:  *Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat)?*** | |
| **Date of Issue:**  July 19th 2010 |

**PURPOSE**

To document the procedures to meet PCI compliance requirement 4.2

**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.

All paper and electronic media that contain credit cardholder information should be physically secured at all time.

**PERSONNEL INVOLVED**

Director

All Management and Supervisors

Parking Office Staffs

Parkade Attendants

**CONTACT INFORMATION**

For policy enquiries, please contact Senior Financial Management at 2-4815.

**PROCEDURE**

1. Phone Communication: paper form with credit cardholder information is used for either sales or charge inquiry purpose. Credit cardholder information should be recorded on the Standard Form. The form should be stored in a secured storage cabinet (locked drawer or file cabinet) until needed for processing. Paper form should be either shredded or kept in locked cabinet after use.
2. Email Communication: at no time should full credit card number be shown in the email communication. The standard format will be 123456xxxxxx1234 + Service Code + Expiry Date. Customers should be strongly encouraged not to give out full credit card number in emails. Any email received that has credit cardholder information on it must be printed and the email deleted immediately. The printed email should be stored in a secured storage cabinet (locked drawer or file cabinet) until needed for processing and should be either shredded or kept in locked cabinet after use.
3. Fax Communication: customers should be strongly encouraged not to give out full credit card number on fax. Any fax received that has credit cardholder information on it should be stored in a secured storage cabinet (locked drawer or file cabinet) until needed for processing. Fax copy should be either shredded or kept in locked cabinet after use.
4. Manual Imprint of Cardholder Information: these will only occur due to off-site sales where wireless application can not occur or technological problems arise that prevent direct entry into payment card terminals. The merchant copy of the manual imprint of credit cardholder information should be stored in the POS or locked in cash drawer until the end of business day. The information is then transferred to Parking Office for secure filing. The imprint copy will be shredded after the required storage period.

**REVISION HISTORY**

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