PCI DSS Requirement 11.1:

Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

Note: *Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*

UBC PCI Procedures:

- PCI DSS requires conducting inspection on a quarterly basis of authorized and unauthorized wireless access points.
- The physical inspection is to complement the wireless Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) provided and maintained by UBC IT.
- Walk around the perimeter of the merchant's place and observe if there is anything strange out of normal.
- Detect unauthorized wireless devices that may be hidden within or attached to a computer or other system component, or be attached directly to a network port or network device, such as a switch or router.
- Ensure that you document the date and time of the inspection/assessment, the person who did the inspection/assessment, rogue access points detected, if any, and action taken to remediate any rogue access point.

Merchant is responsible to report to UBC IT any identified unauthorized access points:

1. A rogue access point (AP) is either discovered by UBC IT through its management system or receipt of report from a UBC staff member.
2. UBC IT will attempt to remotely locate the rogue access point and determine if it is connected to a switch port on UBC's network by performing a switch port trace.
3. Once UBC IT determined the room location, switch port CCT, etc ., they will forward the issue to the LAN admin responsible for that area and request that it be shut down as per UBC security policy and Policy # 130, 3.2 (Management of the Wireless Network).
4. If the AP cannot be located remotely then UBC IT will perform a site visit with its tracking equipment to determine its location and threat level and apply the UBC security policy and Policy # 30 as deemed appropriate.

Assessment: (Please use extra sheet if required, for multiple locations)

Location/Remarks	Yes	None	N/A	Access Points
				WLAN cards inserted into system components
				Portable or mobile devices attached creating wireless access point, e.g by USB
				Wireless devices attached to a network port or network device
				WLAN cards inserted into system components
				Portable or mobile devices attached creating wireless access point, e.g by USB
				Wireless devices attached to a network port or network device
				WLAN cards inserted into system components
				Portable or mobile devices attached creating wireless access point, e.g by USB
				Wireless devices attached to a network port or network device

Merchant's Compliance Attestation:

I attest that _____ is in compliance with the PCI DSS Requirement 11.1 on physical inspection and assessment of rogue access points. The rogue access point inspection/assessment has been conducted over the period of _____ by _____.

_____ _____

Merchant Signature Date