PowerCloud Systems PCI DSS 2.0 Compliance Overview

- PowerCloud Systems utilizes the Amazon Elastic Computing (EC2) cloud platform. All Amazon datacenters are PCI-DSS compliant.
- PowerCloud Systems cloud controller is out of band. Thus, wireless traffic (including card holder data) does not flow through the cloud controller.
- The PowerCloud Systems' cloud managed access point agent, CloudCommand, utilizes SSL technology with X509 security certificates, generated upon manufacturing, to authenticate each access point uniquely and guarantee encryption of all the control traffic to and from the CloudCommand server. These approaches eliminate the risk of spoofing or man-in the middle attacks targeting the control plane, facilitating the utilization of cloud-controlled access points in PCI compliant data networks.
- PowerCloud Systems' built in firewall (client isolation) can be configured to deny any wireless traffic on the local LAN or cardholder data environment (CDE). Client isolation must be turned on for all SSIDs.
- VLAN segmentation with separate gateway termination can be employed to further isolate CDE from wireless traffic.

The following table lists how PowerCloud Systems products meet specific PCI requirements:

PCI Requirement		How PowerCloud Systems Meets the Requirement
1.2.3 Install perimeter firewalls between any wireless network and the CDE, and configure these to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment to the CDE.		This is considered an industry best practice even for non-segmented networks. PowerCloud Systems built-in firewall allows for both LAN and client isolation for each of the SSIDs in the network.
2.1.1 For wireless environments connected to the CDE or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.		PowerCloud Systems does not ship with any default keys that need to be changed. All wireless security settings are enabled for strong encryption. All management control is secured with SSL utilizing X509 security certificates.
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the CDE, use industry-standard practices (for example, IEEE 802.11i) to implement strong encryption for authorization and transmission.		PowerCloud Systems products utilize WPA2-PSK and WPA2-Enterprise (IEEE 802.11i) with AES encryption.
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.		PowerCloud Systems provides the latest firmware for the APs in use via the cloud-based delivery. Enable has the ability to force all APs to update to the latest firmware.

7.2 Establish an access control system for system components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.		PowerCloud Systems provides multiple levels of access control across an implementation. These roles include full, limited, or no ability to view or change network and AP settings. Further, access to individual access points is password protected.
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.		While this is the implementer's responsibility, Enable APs come with a steel reinforced Kensington slot for securing the AP. Additionally, APs can be placed above a suspended ceiling for further security.
10.5.4 Write logs for external facing technologies onto a log server on the internal LAN…verify that logs for the external facing technologies are offloaded or copied onto a secure centralized internal log server media.		PowerCloud Systems' event logs are automatically stored securely in the cloud. Event logs may be reviewed, filtered, and exported to any appropriate media.
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection systems(IDS) and authentication, authorization, and accounting protocol (AAA) servers.		PowerCloud Systems provides centralized monitoring and logging of all devices attempting wireless access in the detailed event log.
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.		Rogue AP detection is available both on demand and via a scheduled process. The facility to identify known versus unknown access points is also included.
12.3 Develop usage policies for critical employee-facing technologies (for example, remote access technologies, wireless technologies…) to define proper use for these technologies for all employees and contractors.		Implementer's responsibility.
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.		PowerCloud Systems provides alerts via email and SMS, as well as logging these events in the event log.