

## PCI Data Security Standard Twelve Requirements

The PCI DSS holds restaurant operators and retailers accountable for being compliant. Using a Payment Application Data Security Standard-validated payment application helps businesses get one step closer to achieving compliance, but is not the only requirement for PCI compliance.

Category	Requirements	Radiant vs. Customer-Managed
<b>Build and Maintain a Secure Network</b>	<ul style="list-style-type: none"> <li>• Install and maintain a firewall configuration to protect cardholder data</li> <li>• Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ul>	<b>Customer</b>
<b>Protect Cardholder Data</b>	<ul style="list-style-type: none"> <li>• Protect stored cardholder data</li> <li>• Encrypt transmission of cardholder data across open, public networks.</li> </ul>	<b>Customer &amp; Radiant</b> - Aloha POS has been validated against the Payment Application Data Security Standard. Validated versions ensure that full credit card track is not stored in any form after authorization is complete.
<b>Maintain a Vulnerability Management Program</b>	<ul style="list-style-type: none"> <li>• Use and regularly update anti-virus software</li> <li>• Develop and maintain secure systems and applications</li> </ul>	<p><b>Customer</b> – Responsible for ensuring that all system components and software have the latest vendor-supplied security patches installed within one month of release (all vendors who have software deployed on systems – operating system, anti-virus, Aloha, etc.)</p> <p><b>Radiant</b> – Responsible for developing a PA DSS validated payment application and providing security updates to the payment application within one month of a vulnerability being identified.</p>
<b>Implement Strong Access Control Measures</b>	<ul style="list-style-type: none"> <li>• Restrict access to cardholder data by business need-to-know</li> <li>• Assign a unique ID to each person with computer access</li> <li>• Restrict physical access to cardholder data</li> </ul>	<b>Customer</b>
<b>Regularly Monitor and Test Networks</b>	<ul style="list-style-type: none"> <li>• Track and monitor all access to network resources and cardholder data</li> <li>• Regularly test security systems and processes</li> </ul>	<p><b>Customer</b> – Responsible for managing the audit logs for payment applications and system components.</p> <p><b>Radiant</b> – Responsible for providing audit logging for the payment application</p>
<b>Maintain an Information Security Policy</b>	<ul style="list-style-type: none"> <li>• Maintain a policy that addresses information security</li> </ul>	<b>Customer</b>