



CARDHOLDERS SECURITY

Driclad Pool Technology Pty Ltd adhere to the Payment Card Industry (PCI) Data Security Standards (DSS). These are a set of standards that must be followed when accepting, storing, processing and transmitting customer's credit card information. The following requirements are followed by Driclad Pool Technology Pty Ltd for PCI compliance:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters. Always change vendor-supplied defaults before installing a system on your network
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks. Use strong cryptography and security protocols
5. Use and regularly update antivirus software. Make sure that your antivirus software remains current and actively running
6. Develop and maintain security systems and applications
7. Restrict access to cardholder data by business employees on a need-to-know basis only
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security