PCI Data Security Standard

Notes

This is a High Level Overview of the PCI Data Security Standard which all organisations that request or are provided with credit card data must comply with. More detailed information can be found on the PCI-DSS website.

Standard	Compliance	Pegasus Response
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data	Pegasus' ICT system provider regularly updates the firewall to protect its electronic information. Pegasus does not store cardholder data. Once payment card information is used for the purpose for which it was collected it is deleted (soft-copy) or placed in confidential waste (hard-copy).
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	Pegasus does not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data	Pegasus does not store cardholder data.
	4. Encrypt transmission of cardholder	Pegasus does not transmit cardholder data across open public

Standard	Compliance	Pegasus Response
	data across open, public networks	networks. Online credit card donations are processed using the Our Community GiveNow system which uses state-of-the-art encryption software. Other credit card donations are processed manually using our mobile credit card facility or our online merchant facility, Secure Pay. In both cases, the card details are secure because the card is returned or the donation voucher is disposed of in a locked confidential waste bin.
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs	Pegasus' ICT system provider regularly updates anti-virus and similar software and systems protection programs. This is part of their service contract
	6. Develop and maintain secure systems and applications	Pegasus' ICT system provider develops and maintains secure systems and applications. This is part of their service contract
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know	Pegasus does not store cardholder data electronically. Once payment card information is used for the purpose for which it was collected, it is deleted (soft-copy) or placed in confidential waste (hard-copy).
	8. Identify and authenticate access to system components	All people accessing the Pegasus System must authenticate their identity through the use of user names and passwords. Users' access to particular components of the system is limited to those who need access to that component in order to effectively

Standard	Compliance	Pegasus Response
		perform their job.
	9. Restrict physical access to cardholder data	Pegasus' does not physically or electronically store cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	Pegasus' does not physically or electronically store cardholder data.
	11. Regularly test security systems and processes	Pegasus' ICT system provider regularly tests security systems and processes. This is part of their service contract.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel	Pegasus maintains a policy that addresses information security for all of its stakeholders. This includes staff, volunteers, riders, donors, friends, and suppliers.