PCI DSS Policy

1.Overview

This policy sets out the requirements which are necessary to protect the security of all payment card details that are received and processed by Gemporia which are governed by the Payment Card Industry – Data Security Standard (PCI DSS). Compliance with PCI DSS is mandatory for any company or organisation which stores, processes or transmits payment card data. Failure to comply with these requirements could result in data breaches leading to Gemporia being fined by the acquirer with the need for additional controls implemented and losing customers.

2.Responsibility for Maintenance

The Gemporia IT Director is responsible for ensuring that this document is kept current for the purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives. The document must be reviewed and updated at least annually with the updated version rolled out to all concerned personnel.

3.Scope

This policy applies to all the assets that are covered as per the Gemporia’s Card Holder Environment (CDE).

4.Policy

It is the policy of Gemporia to ensure that all payment card details received and processed by the company is done in accordance with the requirements of the PCI DSS standard. It must be ensured that

1. Card details must only be sent or received via the approved channels.
2. The channels used to receive card details must be secured as per the industry best practices.
3. The payment card details must not be captured on any magnetic/ paper mediums by Gemporia staff.
4. Any medium containing the full card number must be secured at all times.
5. Card numbers if displayed must be masked to display not more than the first six and last four digits.
6. Card details must never be transmitted using emails or any other insecure messaging technologies.
7. All electronic/paper media containing cardholder details must be securely destroyed at the end of their retention period.
8. All incidents reported to affect the security of cardholder’s environment (CDE) must be investigated.

9. Any hard copies containing the full 16 digits of the card number (PAN) must be secure stored such as in a locked cabinet or safe.
10. No unauthorised devices are connected to the CDE and a change control process must be followed for any changes affecting the security of CDE.
11. Only authorised staffs have access to Gemporia's cardholder environment.
12. Written agreements must be in place for all third party contractors/ vendors who interact/ support Gemporia's cardholder environment.
13. Annual penetration tests are conducted both externally and internally to identify and address evolving vulnerabilities.
14. Cardholder environment is adequately segregated from the rest of the network.
15. Physical security to all areas processing cardholder data must be ensured.
16. Policies and supporting documents exist to cover all areas as required by the PCI DSS standard.
17. All access to the Cardholder Data Environment must be restricted to authorised personnel. All visits must be recorded and be by pre-approved staff only. Physical access to hardware must be restricted with appropriate controls. Approval for access to the PCI CDE environment must be granted by the Director for IT
18. Proper due diligence must be conducted before involving new 3rd parites who may store CHD on our behalf
19. All new hardware and software for the CDE must have all factory default settings disabled, removed or changed before installation onto the network
20. All new hardware and software for the CDE must have all surplace services and protocols disabled and be configured as per the server setup standard
21. Wireless hardware is not permitted in the CDE
22. PCI task list is to be reviewed daily and completed within 1 week of due date
23. All CDE technologies are to be contained within the secured CDE environment, this relates to both the physical location as well as the network level security

5.Conclusion

This document is aimed at providing the high level statements with regards to Gemporia's PCI compliance and must be supported by other relevant policies, procedures and processes as deemed necessary.

6.Revision History

Date	Description	Who
12/10/2014	Original Document	Andrew Smith
13/10/2015	Added physical access details	Andrew Smith
20/11/2015	Added 4.18	Andrew Smith
30/11/2015	Added 4.20 and 4.19	Andrew Smith
01/12/2015	Added 4.21 explicitly	Andrew Smith
01/12/2015	Updated 4.6 to include all messaging technologies	Andrew Smith
23/02/2016	Review, no change	Andrew Smith
24/05/2016	Changed TGGC to Gemporia	Andrew Smith
24/08/2016	Review, no change	Andrew Smith
07/11/2016	Added requirement for staff to be approved by Director for IT before being granted access to CDE	Andrew Smith

Date	Description	Who
24/11/2016	Review, no change	Andrew Smith
24/02/2017	Review, no change	Andrew Smith
24/05/2016	Review, no change	Andrew Smith