PCI DSS – Wireless Hardware Policy

1.Overview

This policy covers wireless hardware used within the CDE, either authorised or unathorised

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 document applies to the people, processes and technology that store, process or transmits cardholder data or sensitive authentication data, including systems that produce logging information and any connected system components. This includes contractors, vendors and any other personnel that have may have an impact on the cardholder data environment.

4.Policy Statement

- Gemporia does not allow unauthorized wireless hardware within the CDE.
- Any unauthorized wireless hardware detected shall be classified as a data breach incident and the procedure for handling this shall be followed according to the Data Incident Response document
- Quarterly wireless scans shall be conducted for unauthorized wireless hardware
- Wireless scans shall include a visual check of all ports on servers, routers, firewalls and switches and utilisation of a wifi scanning app or hardware to show any unauthorised wifi networks

5.Glossary

The purpose of the following glossary is to communicate the meaning of specific PCI DSS terminology used in this document. The official PCI DSS Glossary issued by the Payment Card Industry Payment Security Standards Council has been the source of the definitions used below.

Cardholder Data: At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See Sensitive Authentication Data for additional data elements that may be transmitted

or processed (but not stored) as part of a payment transaction.

Cardholder Data Environment (CDE): The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

Wireless Hardware: Any network component capable of establishing a wireless network connection to the CDE, including but not limited to wireless access points, bridges and routers

Revision History

Date	Description	Who
12/10/2015	Original Document	Andrew Smith
05/01/2016	Review: No change	Andrew Smith
05/04/2016	Review: No change	Andrew Smith
04/10/2016	Change TGGC to Gemporia	Andrew Smith
04/01/2017	Reviewed, no changes	Andrew Smith
04/04/2017	Reviewed, no changes	Andrew Smith
04/07/2017	Reviewed, no changes	Andrew Smith