Transport for Greater Manchester

Transport for Greater Manchester Policy

# P04 IS Wireless Policy

## Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

| | | | |
|---|---|---|---|
| Date Prepared: | 25th March 2020 | Document<br>Reference no. | IS Wireless Policy<br>P04 |
| Version No. | 5.0 | Prepared by: | Claire Styler, Catherine Burke & Rohan Mendis |
| Equality Impact Assessment | Validation of Initial Screening<br>Equality Officer: Muhammad Karim<br>**Date:** | | Full Impact Assessment completed: YES<br>**Validated by Equality Officer signature:**<br>**Date:** |
| Authorisation Level required: | Executive Group/Director | | Staff Applicable to:<br>All Staff |
| Authorised by:<br>Date: | Head of IS Operations (Ricard Fuertes)<br>31st March 2020 | | Implementation date:<br>31st March 2020<br>Annual review date:<br>31st January 2021 |

## Table of Contents

1 Policy Aims ........ **3**

2 Review and Update of the Policy Statement ........ **3**

3 Purpose ........ **3**

4 Scope ........ **3**

5 Policy Delivery ........ **4**

6 Accountability ........ **4**

7 Enforcement / Monitoring / Compliance ........ **4**

8 Policy ........ **4**

8.1 General Security ........ 5

8.1.1 Hardware ........ 5

8.1.2 Software ........ 5

8.1.3 Testing and Updates ........ 6

8.2 Configuration ........ 6

8.2.1 Network Segmentation ........ 6

8.2.2 Security ........ 6

8.3 Password Changes ........ 7

8.4 Acceptable Use ........ 7

8.5 Access to Sensitive Materials ........ 7

8.6 Third Party to Wireless Networks ........ 8

8.7 Access Points / Wireless Bridges ........ 8

8.8 Signal Emanation ........ 9

9 Glossary and References ........ **9**

9.1 Glossary ........ 9

9.2 References ........ 9

9.2.1 Policies ........ 9

## 1 Policy Aims

a) This policy details **TfGM's** policy for wireless networking and access to resources via wireless networks.

b) The policy is aimed specifically at Wireless Networks and related Access for the networks that store, process or transmit **TfGM's** payment card data.

c) This document should be viewed in conjunction with **TfGM's** top level security policy P01 – IS Information Security Policy.

## 2 Review and Update of the Policy Statement

a) The policy statement and associated **TfGM** Policies are reviewed at least annually by **TfGM IS Operations Team** to ensure;

  i) The business meets it compliance obligations to the Payment card Industry Data Security Standard (the PCI DSS). and

  ii) It maintains its relevance to the business' current and planned credit card processing operations.

b) The **IS Operations Team** will undertake the review of this policy statement and associated company policies.

## 3 Purpose

This document details the process used by **TfGM** to ensure PCI DSS compliant use of wireless networks and related access.

## 4 Scope

a) This document details the Policy that has to be adhered by members of **TfGM** staff and third parties that intend to use **TfGM's** wireless network(s).

b) The policy covers the components that forms a wireless network, including wireless access points, wireless routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

c) For the purpose of PCI DSS compliance, only wireless access that is contained in the card holder data environment is in scope.

d) Networks in Scope

| Network Name | Description |
|---|---|
| Nil | There are no wireless networks deployed in the TfGM CDE |

## 5 Policy Delivery

This policy will be delivered to **TfGM** IS Staff by internal communication and will be situated on the **TfGM** Intranet.

## 6 Accountability

- **Responsonible to board:** Head of IS Operations
- **Compliance:** All
- **Awareness:** All

## 7 Enforcement / Monitoring / Compliance

a) This policy will be enforced by the Executive.

b) Information including dates, times, duration and device identity will be logged and maybe used for monitoring purposes, and may be used in disciplinary proceedings.

c) Should a breach or violation of this policy be identified, it may result in disciplinary action in accordance with **TfGM** disciplinary policy.

## 8 Policy

a) Use of any wireless equipment in the **TfGM** cardholder data environment is prohibited.

b) If **TfGM** were to implement wireless access points or wireless bridges in the CDE then the relevant section of this policy shall apply.

## 8.1 General Security

a) On wireless networks transmitting cardholder data, or connected to the CDE, the authentication transmissions must be strongly encrypted.

b) All authorised staff and third parties must not disclose details about the configuration of the wireless network to anyone, without prior permission from the **Head of IS Operations**.

c) All authorised staff and third parties must report attempts by people to obtain information about the wireless network or wireless security systems to a member of the **TfGM's IS Operations Team**.

d) Should authorised staff/third parties observe a person or persons acting suspiciously with Wireless Networking Equipment or Computing Hardware, they must report it to the **TfGM's Head of IS Operations.**

e) At **TfGM** only the approved wireless networks shall be used.

f) Before wireless technology is implemented, **TfGM** will carefully evaluate the need for technology against the risk, and consider more secure alternatives if feasible.

### 8.1.1 Hardware

a) **TfGM** will only deploy wireless products specified in the Cisco Unified Access Solution to create the wireless infrastructure in the **TfGM** CDE.

b) Wireless hardware must be configured to insist upon IEEE 802.11i (WPA2) encryption and authentication. Use of WEP is prohibited.

### 8.1.2 Software

Client software must support IEEE 802.11i (WPA2) and encryption and authentication to gain access to the wireless network(s). Use of WEP is prohibitied.

### 8.1.3 Testing and Updates

a) Hardware and Software shall be reviewed on a Six (6) monthly basis and any deficiencies corrected, as soon as the vendor fix is available.

b) **TfGM** will conduct tests using a wireless analyser or at least quarterly to test for rogue wireless access points (see P02 – IS Security Audit Policy, section 8.5 Wireless Access Scans). This is conducted even if **TfGM** does not operate an approved wireless network.

**Note:** The use of continuous monitoring solution is permitted as an alternative. If this is used, update the above accordingly, and see P02 – Audit Policy Section 8.5 Wireless Access Point Scans

## 8.2 Configuration

### 8.2.1 Network Segmentation

a) **TfGM** will only deploy wireless technology where it is considered unfeasible or prohibitively expensive to place physical connections.

b) Perimeter firewalls shall be installed and configured to segment the wireless networks from the CDE.

c) All traffic between cardholder data environment and the wireless network must be denied unless required for business purposes.

### 8.2.2 Security

a) **TfGM** will ensure that the wireless implementation team remove default settings for access points (e.g. vendor default encryption keys, passwords / passphrases, SSID, configuration utilities, SNMP Community Strings) are either removed or changed.

b) In addition, firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks.

c) Encryption keys must be changed every time a staff member with knowledge of the encryption keys leaves or changes position.

d) All wireless devices must to be kept updated to support strong encryption for authentication and transmission.

e) All access points / wireless bridges will be purchased from the approved hardware vendor and must conform to the security access requirements.

f) The firewalls shall be configured to either deny or control any traffic from the wireless environment on the CDE.

g) Access Points/Wireless Bridges will be configured to use WPA-2 with strong wireless encryption with keys of 256 length.

h) **TfGM** will not implement any new wireless network using Wired Eqivalent Privacy (WEP), which is prohibited under PCI DSS v3 onwards. For current wireless implementations, it is prohibited to use WEP (deadline was June 30, 2010).

i) Web based Configuration Interfaces shall be configured to only allow connections via TLS or SSLv3 or higher. Telnet and other insecure remote log-in commands must not be available for use for administration login.

j) Only the **IS Team** will have access to configure the Wireless Bridge/Wireless Access Point.

### 8.3 Password Changes

Passwords must be changed in accordance with the company password policy (P05 - Operational Policy, Section 8.4.3).

### 8.4 Acceptable Use

The Wireless Network is governed by the rules detailed in P06 - Acceptable Usage Policy.

### 8.5 Access to Sensitive Materials

a) **TfGM** will ensure that, as well as the encrypted Access Point / Wireless Bridge, that a point-to-point VPN is implementated to further encapsulate and protect data that travels over the Access Point /  Wireless Bridge.

b) **TfGM** will ensure that only those systems that require access to the Access Point / Wireless Bridge can access it and that all other systems are expressly denied.

8.6 Third Party to Wireless Networks

a) Access by Third Parties to the **TfGM** wireless network is at the discretion of the **Head of IS Operations**.

b) Third Party Access to the Sensitive Network via the Wireless VPN Router is only allowed at the discretion of the Head of IS Operations.

8.7 Access Points / Wireless Bridges

a) **TfGM** shall maintain an inventory of authorised wireless access points.

b) **TfGM** shall have a documented business justification for all authorised wireless access points.

c) Only the **TfGM's IS Operations Team** (under the authorisation of the **Head of IS Operations**), may install Wireless Access Points on all system components within cardholder data environment, and any rogue devices found must be investigated.

d) The **TfGM IS Operations Team** conduct quartley searches for unauthorised wireless access points on all system components within cardholder data environment, and any rogue devices found should be investigated. The output of the tests and any investigations required should be fully documented and reported to **TfGM's** IS Operations Team. Wireless Access Points /  may be configured as follows:

- WLAN cards inserted into system components.
- Portable devices connected to system components.
- Wireless devices attached to a network port or network device.

e) Methods which may be used to detect unauthorised wireless access points include network scans, physical / logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS / IPS device.

f) Users found to have installed such hardware without clearance will be subject to an investigation and disciplinary action.

8.8 Signal Emanation

**a)** **TfGM** will ensure that all access points conform to all relevant broadcast regulations within the relevant legal jurisdiction and will be at the minimum required to provide wireless coverage within the target area.

**b)** **TfGM** will ensure that signal emanation outside of **TfGM** locations into public areas is minimised.

## 9 Glossary and References

9.1 Glossary

- See document P99 - Glossary

9.2 References

9.2.1 Policies

- P01 - IS Security Policy
- P02 – IS Security Audit Policy
- P05 – IS Operational Policy
- P06 – IS Acceptable Usage Policy

| Policy: IS Wireless | | | | |
|---|---|---|---|---|
| **Version** | **Change** | **Reason for change** | **Date** | **Name** |
| 1.1 | Date | Review and Update | 30/10/2013 | C.Burke |
| 1.2 | Date and version | Annual update | 06/03/2014 | C. Burke |
| 1.3 | Update | Updated to include Version 3.0 change variations. | 16/02/2015 | C.Burke |
| 1.4 | IS Director to Head of IS | IS Director left the organisation | 11/05/2015 | C Burke |
| 2.0 | Department name change | Department name change | 10/08/15 | J.Singleton |
| 2.1 | Date and Version | Annual Update | 31/03/2016 | C. Burke |
| 2.2 | Date and Version | Annual Review | 31/03/2017 | C. Burke |
| 3.0 | Date and Version | Annual Review | 31/03/2018 | C. Styler |
| 4.0 | Update & Annual Review | Changed IS Infrastructure Manager to Head of IS | 18/02/2019 | C. Styler |
| 4.0 | No Change | Annual Review | 11/03/2019 | C.Burke |
| 5.0 | Annual Review & Update | Changed Head of IS to Head of IS Operations and change of IS Team to IS Operational Team | 25/05/2020 | C. Styler |