Transport for Greater Manchester Policy

# P11 – IS Systems & Applications Development Policy

## Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

| | | | |
|---|---|---|---|
| Date Prepared: | 11th March 2019 | Document<br>Reference no. | IS Systems & Applications Development Policy<br>P11 |
| Version No. | 4.0 | Prepared by: | Catheirne Burke/Rohan Mendis |
| Equality Impact Assessment | Validation of Initial Screening<br>Equality Officer: Muhammad Karim<br>**Date:** | | Full Impact Assessment completed:<br>YES<br>**Validated by Equality Officer signature:**<br>**Date:** |
| Authorisation Level required: | Executive Group/Director | | Staff Applicable to:<br>All Staff |
| Authorised by: | Head of IS (Malcom Lowe) | | Implementation date:<br>31st March 2019 |
| Date: | 31st March 2019 | | Annual review date:<br>31st January 2020 |

## Table of Contents

## Policy Aims

a) This document details **TfGM’s** policy in relation to development of networks and applications that handle the storage, processing and transmission of payment card data.

b) This document should be viewed in conjunction with **TfGM’s** security policy: P01 - IS Security Policy.

## Review and Update of the Policy Statement

a) The Policy Statement and associated company Policies are reviewed at least annually by **TfGM IS Team** to ensure:

- the business meets its compliance obligations to the PCI DSS; and
- it maintains its relevance to the business’ current and planned payment card processing operations.

b) The **TfGM IS Team** shall undertake the review of this policy statement and associated company Policies.

c) Any changes to this policy document will be communicated to all members of **TfGM’s IS Team**.

## Purpose

a) **TfGM** recognises the importance of thoroughly testing all application and network changes prior to release in the live/production environment.

b) Secure code and secure supporting software products are essential for **TfGM** requirements to avoid large-scale payment card data compromise.

## Scope

a) This document details the guidelines used at **TfGM** to ensure application and network changes to the cardholder data environment are tested and planned to the best of **TfGM** abilities prior to release.

b) These guidelines have been developed according to the standards as set by the Payment Card Industry Data Security Standard (PCI DSS).

c) This document provides operational guidelines for individuals performing application and network development for card processing networks at **TfGM**. These guidelines are applicable to (and is not limited to):

- Permanent members of staff.
- Contract members of staff.
- Third Party Service Providers.
- Site Visitors

**Policy Delivery**

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

**Accountability**

- **Responsible to the Board**: Head of IS
- **Compliance**: All
- **Awareness**: All

**Enforcement /Monitoring / Compliance**

a) These guidelines are in place to secure **TfGM'**s Systems and Applications development activities.

b) Adherence to these guidelines shall be monitored on a regular basis to ensure all Systems and Applications development activities are protected,

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

## Policy

### 8.1 Systems Division

### 8.1.1 Separation of Duties

a) Where possible, **TfGM** shall maintain a distinction between the staff responsible for applications development and those responsible for administering production systems.

b) Should it not be possible to achieve such separation, then staff shall have separate accounts for development work and administration work.

### 8.1.2 Separation of Environments

a) **TfGM** shall ensure that a clear division is in place between the development / testing and live systems used by **TfGM**. Each environment shall be located on physically separate machines.

b) Each environment shall be on physically separated networks (either through physically distinct cabling or through VLAN segregation). Each shall also be separated by a firewall to ensure that traffic from one network cannot reach any of the others.

c) Production Cardholder Data must under no circumstances be used on the development/testing environments.

d) Where testing requires the use of 'live' data, cardholder data shall be replaced with test cardholder data in all instances, before installation on the test system.

### 8.2 Development Best Practice

### 8.2.1 Database Access

a) Any applications developed by or on behalf of **TfGM**, shall ensure that direct SQL queries are disallowed for all staff, with the exception of systems administrators. Where possible, restrict systems administrator privileges to the least required for day-to-day operations.

b) All connections to the database system must be authenticated. This includes access by individual users, administrators, and applications.

c) ID's set up for application should only be used by applications and not individual users.

d) Ensure that database and application configuration settings ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).

8.2.2 Cardholder Data

a) If Card Data is being stored for any period of time, controls must be applied to that data using one or more of the following techniques:

i) Encryption, using an industry-recognised secure encryption algorithm

ii) Truncation, retaining at most the first 6 and last 4 numbers only

iii) Hashing, using a secure one-way hashing algorithm with a salt.

iv) Index tokens and pads, with the pads being securely stored.

b) When displaying a PAN, only the first 6 and last 4 digits of the Card Number are to be displayed. Where full card numbers are required for business reasons, **TfGM** ensures that viewing of cardholder data can be traced to an individual user.

c) Samples should be taken from data repositories, removable media, audit logs containing PAN data to ensure that the PAN is rendered unreadable.

d) Cardholder data stored for any length of time shall only be held provided it meets the obligations laid down in PR10 - Data Retention Procedure.

e) Refer to the preface of the PCI Data Security Standard, on page 2, which details the controls needing to be placed upon each cardholder data element, and which elements may not be stored post-authorisation even with controls applied.

8.2.3 Industry Best-Practice Development Guidelines

a) **TfGM** ensures that software development processes follow recognised industry standards and take into account the prevalent threats to e-commerce and IT infrastructure, such as standards by OWASP and SANS.org (see http://www.owasp.org & http://www.sans.org/).

b) **TfGM** shall ensure that all developers are given adequate training in issues relating to IT security and secure applications development.

8.2.4 Non Consumer Passwords

a) **TfGM** shall ensure that all non-consumer passwords adhere to its password policy.

b) **TfGM** shall ensure that non-consumer customers are informed of its password policy (e.g. as documentation in a web application.

Policy regarding non-consumer users id documented in **P05 – Operational Policy, 8.3.13 Password/Session Lockout and Resetting.**

8.3 Testing Strategies

a) Code testing shall make specific provision for the detection (and resolution) of the following issues:

(i) Cross Site Scripting (XSS).

(ii) SQL/OS Command / LDAP / XPATH Injection Flaws etc.

(iii) Buffer Overflow.

(iv) Cross Site Request Forgery (CSRF).

(v) Information Leakage and Improper Error Handling.

(vi) Insecure Cryptographic Storage.

(vii) Insecure Communications.

(viii) Improper Access Control.pci

(ix) All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2) Note: This requirement is considered best practice until June 30, 2012, after which it becomes a PCI DSS requirement.pci.

b) During development, **TfGM** requires developers to write unit tests to further assist higher level testing of code. Emphasis should be placed on testing for protection against the above issues.

c) All code shall undergo integration testing and code review (see Section 8.4) prior to deployment.

d) For each functional change, functionality tests must be conducted to ensure the code developed performs the function it is expected to perform. This should be done with reference to the original specification.

e) The **TfGM's Development Team** shall ensure that test and custom data is removed from the system prior to deployment.

f) Customer Applications accounts, user ID's and passwords created on the host for testing purposes shall be removed prior to deployment.

## 8.4 Code Reviews & Web Application Firewalls

Code reviews must be conducted when new code is to be added, or when changes are made to an existing codebase, as well as when changes are made to existing codebases.

Code reviews must be completed prior to release to production or to customers, in order to identify any potential coding vulnearabilities.

8.4.1 Use of Automated Tools:

a) Where possible, automated tools are used to detect vulnerability issues in the code.

b) Results generated by automated review tools must be given to another member of the development team to review and manually inspect the code.

8.4.2 Code Inspections:

Manual code inspections must be conducted following an automated review by a suitably-qualified programmer knoweledgeable in code review techniques and secure coding practices who was not involved in writing the code being reviewed.

8.4.3 Code Failing Review

a) Code which fails review shall be returned to the developer with a list of appropriate modifications. When the modifications are completed, the code shall be re-submitted to the review process.

b) Code which passes review shall be approved by management prior to release.

8.4.4 Relation to Code Testing

a) Code reviews shall be conducted following the code testing process and prior to functionality testing.

b) For public-facing web applications, address new threats and vulnerabilities on an on-going basis and ensure these applications are protected against known attacks by either of the following methods:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes, or

- Installing a web application firewall in front of any public facing web applications.

8.5 Rollout / Rollback Control

a) **TfGM** shall maintain a code repository to track changes made to code by internal developers (or contracted external developers).

b) **TfGM** employs a bug-tracking system to track bugs or faults reported through channels (reports from end users, PCI audit reports etc.) and link them to code written to fix the problem.

c) Code branches intended for deployment to production systems are tested prior to deployment to ensure that the upgrade does not interfere in any apparent way with the production environment.

d) **TfGM** shall ensure that any upgrades to production systems can be rolled back to the previous working version should an issue arise.

8.6 Encryption Technologies

a) **TfGM** ensures that TLS1.2 is used in all cases where credit card data is transmitted over the public Internet. **TfGM** utilises the highest encryption available (128 bit or higher).

b) **TfGM** ensures that at no point is payment card data sent over unencrypted HTTP, under any circumstances.

c) Where SSL client certificates are used, **TfGM** ensures that only trusted certificates are accepted.

d) **TfGM** ensures that TLS 1.2 or better is available on public facing web application servers.

e) **TfGM** ensures that passwords are encrypted or hashed during storage and transmission.

f) Where passwords are issued by **TfGM** to customers, observe password files to verify that customer passwords are encrypted (for service providers only).

## 8.7 Software Development Lifecycle

a) **TfGM** documents the Software Development Lifecycle methodology in use and ensure that new staff  are trained in working to the methodology.

b) Ensure that Information Security is considered and included in the Software Development Lifecycle as appropriate, and develop applications adhere to PCI DSS.

## 8.8 Code Migration into Production Environment

a) All Production network and application changes applied to **TfGM**'s cardholder data environment must be documented and agreed using Change Control requests. More information on change control request forms can be obtained from the following team: Change Control team.

b) All changes are formally signed off before migration to the cardholder data environment(s).

c) Test data and accounts will be removed before production systems become active.

## Glossary & References

### 9.1 Glossary

See document P99 - Glossary

### 9.2 References

- P01 – IS Security Policy
- P05 – IS Operational Policy
- PR10 – Data Retention Procedure

*Change control record: complete each time there is a change*

**P11: Systems and Application Development Policy**

| **Version** | **Change** | **Reason for change** | **Date** | **Name** |
|---|---|---|---|---|
| 1.0 | Date & Version | Annual Review | 31/10/2012 | C.Burke |
| 1.1 | Date & Version | Updated Policy | 31/10/2013 | C.Burke |
| 1.2 | Date and version | Annual Review | 06/03/2014 | C. Burke |
| 1.3 | Update | Updated to include Version 3.0 change variations | 16/03/2015 | C. Burke |
| 1.4 | Date and Version | Annual Review | 31/03/2016 | C. Burke |
| 2.0 | Inclusion of TLS1.2 protocol and removal of all other encryption protocols | Achieve PCI DSS V3.2 compliance | 12/01/2017 | C Burke |
| 3.0 | Date & Version | Annual Review | 31/03/2017 | C. Burke |
| 4.0 | Date & Version | Annual Review | 11/03/2019 | C. Burke |