Transport for Greater Manchester

Transport for Greater Manchester Policy

P05 – IS Operational Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31st March 2021	Document Reference no.	IS Operational Policy P05
Version No.	7.0	Prepared by:	Catherine Burke/Rohan Mendis
Equality Impact Assessment	Validation of Initial Screening Equality Officer: Muhammad Karim **Date:**		Full Impact Assessment completed: YES **Validated by Equality Officer signature:** **Date:**
Authorisation Level required:	Executive Group/Director		Staff Applicable to: All Staff
Authorised by: Date:	Head of IS Operations (Ricard Fuertes) 31st March 2021		Implementation date: 31st March 2021 Annual review date: 31st January 2022

Table of Contents

1 Policy Aims

a) This document details the **TfGM** policy for daily operational procedures concerning the Card Data Network (CDE). The CDE includes all components that store, process or transmit cardholder data, or are connected to such systems.

b) This document Lists the security standards and procedures required to maintain **TfGM's** cardholder data environments to the required standard as set by Payment Card Industry standards.

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

2 Review and Update of the Policy Statement

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

- The business meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS).
- The policy maintains its relevance to the business' current and planned payment card processing operations.

b) The **TfGM's IS Operations Team**, will undertake the technical review of this policy statement and associated company Policies.

c) Any changes made to this document must be communicated to all members of **TfGM** IS Operations Team and any other affected party.

3 Purpose

This document details guidelines and procedures for members of staff and any third parties that intend to perform network operations within **TfGM's** cardholder data environment.

4 Scope

a) This document provides instruction on maintaining **TfGM's** cardholder data environment to payment Card Industry standards.

b) This Policy is restricted to those employees, companies or contractors that process, store or transmit credit card data on behalf of **TfGM** or have access to such systems.

c) Network(s) in scope:

Network Name	Description
Multi-Service Network – AFC Segment	MacAfee NSP 1450 IDS /IPS Appliance
2PP CDE Firewalls	cde-www.fw01 at 2 Piccadilly Place 2pp-cde-fw01
MSN – 2PP Call Centre Segment	Cisco 2901 Gateway with ISDN E1 trunk

5 Policy Delivery

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

6 Accountability

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

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

8.1 Systems & Security Monitoring

8.1.1 Security Monitoring Systems

a) **TfGM** shall ensure that sufficient technical safeguards are installed and configured to monitor, defend and react to external or internal security threats using the following:

- Firewall and De-Militarised Zone (DMZs) to isolate and protect CDE.
- Intrusion Prevention System or Intrusion Detection Systems.
- File modification monitoring software.
- Automated log backup systems.

Monitoring System	Description
Intrusion Prevention System / Intrusion Detection System **(including wireless IPS/IDS systems where wireless scanning not employed)**	**Product Name:** McAfee NSP 1450 Network Security Platform Appliance. McAfee Network Security Manager Software Standard Edition Perpetual License. **Vendor Contact details:** Lee Baughen Business Development Manager RMS Managed ICT Security Ltd. Innovation House, Bellringer Road, Trentham Lakes South, Stoke on Trent, Staffordshire, ST4 8GH Mob: +44 (0) 782 521 9326 Email: lee.baughen@rmsitsecurity.com

Monitoring System	Description
File Modification monitoring software	**Product name:** McAFee Configuration Control **Vendor Contact details:** Lee Baughen Business Development Manager RMS Managed ICT Security Ltd. Innovation House, Bellringer Road, Trentham Lakes South, Stoke on Trent, Staffordshire, ST4 8GH Mob: +44 (0) 782 521 9326 Email: lee.baughen@rmsitsecurity.com
Log backup systems	**Product name:** Honeycomb Lexicon Enterprise **Vendor Contact details:** John McCann Satisnet Ltd 110 Butterfield Great Marlings Bedfordshire LU2 8DL Telephone +44 (0) 158 243 4320 Facsimile +44 (0) 158 243 4321 e-Mail: John.McCann@satisnet.co.uk

b) Intrusion monitoring system devices and applications must be configured, maintained, and updated per vendor instructions to ensure optimal protection.

c) All IDS / IPS devices should have up-to-date prevention engines, baseline and signatures.

d) All IDS / IP devices should have sufficient capacity, to successfully monitor all traffic at the full throughput of the monitored network. This should be verified with the vendor.

e) **TfGM** shall ensure all traffic at the perimeter of the cardholder data environment is monitored.

f) Details on how the IDS / IPS is configured have been defined in the following IDS / IPS Configuration Standard:

- Configuration of McAfee IDS/IPS Appliances.

8.1.2 Alert Management

a) The **Head of IS Operations** has the responsibility to ensure that security alerts are responded to or relayed to the relevant parties to rectify the situation promptly.

b) Intrusion Prevention System / Intrusion Detection System appliances must be configured to alert personnel of suspected compromises.

c) Upon detection of a security alert, the staff member who receives the alert shall inform the **TfGM Serviceline,** to be forwarded to the **TfGM IS DCS Team.**

d) The **IS DCS Team** will assess whether the alert is genuine, and if so:

- If the alert presents an active threat to the integrity of the network, and
- Does the alert relate to actual/potential disclosure of Sensitive Information from the network?

e) Network integrity threats include (but are not limited to):

- External/internal port scanning
- Rogue processes on network infrastructure
- Hardware/software failures.
- Detection of unauthorised wireless access points.
- Critical IDS alerts.
- Detection of unauthorised critical system or content file changes.

f) Alert Monitoring shall contain the date and time of the alert to allow the **TfGM Serviceline** to ascertain when the alert occurred to aid classification.

g) Security incident response and escalation procedures must be documented and distributed to appropriate members of staff to ensure timely and effective handling of all situations. Refer to P03 - Disaster Recovery & Security Incident Response Policy.

8.1.3 Monitoring IDS/IPS/Web logs

a) The IDS/IPS appliances employed must monitor all traffic at the perimeter of the cardholder date as well as critical points in the card holder data environment.

b) The alerts from IDS/IPS and web logs are forwarded to the log management system Honeycomb.

c) The Honeycomb Log Management System generates a diary report of critical log and diary log reports provided by Honeycomb Log Management System on every business day.

d) The **TfGM IS DCS Team** have procedures in place to monitor alerts forwarded from Intrusion Detection/Prevention Systems (IDS/IPS) and web logs, at least daily.

e) The **TfGM IS DCS Team** shall alert the **Head of IS Operations** should unexpected alerts occur, as defined in PR08 - Security Incident Management Procedure.

8.1.4 Monitoring of **TfGM** Multi Service Network

a) The monitoring of TfGM Multi Service Network shall be done through the use of SNMP Monitoring Utilities.

Monitoring System	Description
Network Monitoring Software employed	**Product name:** Orion Network Performance Monitor - SolarWinds **Vendor contact details:** Chris Morrison Account Manager: BT Engage IT Ltd 3 Midland Way Barlborough Chesterfield S43 4XA Telephone: +44 (0) 124 657 4000 Mobile: +44 (0) 773 428 5658 E-mail: chris.morrison@btengageit.com

b) The Network monitoring utility shall provide the date and time of the alert to allow the **TfGM's IS DCS Team** to ascertain when the alert occurred to aid classification.

8.1.5 Internal Vulnerability Assessment

a) **TfGM** shall ensure internal scans are conducted on a quarterly basis, to determine the security status of the network infrastructure and ensure compliance to PCI DSS requirements.

b) These scans shall include, at a minimum:

- Network & service vulnerability assessments (scans);
- Web application vulnerability assessments.

c) The network and service vulnerability assessment may be achieved by way of the external PCI Quarterly Assessment.

d) Significant changes to the network or applications deployed on the network shall require an additional internal vulnerability assessment.

e) Rescans must be completed until passing results are obtained or until all high vulnerabilities, as defined in PCI DSS Requirement 6.2 are resolved.

f) Internal scans vulnerability scans may be performed by the company's qualified internal personnel or third parties.

8.1.6 External Vulnerability Assessment

a) PCI DSS requires that four quarterly passing external assessments to be completed to achieve and maintain PCI accreditation (see P02 - Audit Policy).

b) On receipt of the external assessment, should there be any areas requiring remediation, the **TfGM Head of IS Operations** shall disseminate the report to the relevant business areas, and ensure that rescans are completed after remediation until passing results are obtained or until all medium and high vulnerabilities are resolved.

c) The quarterly external scans must be conducted by a PCI Approved Scanning Vendor (ASV) (see P02 - Audit Policy).

d) ASV's Details

Approved Scanning	Contact Details	Schedule / Frequency
Claranet Unit 1 Bankwood Way Birstall West Yorkshire WF17 9TB United Kingdom Tel: +44 1924 284240	Matthew Hall Technical Services Manager Sec-1 Ltd Unit 1 Centre 27 Business Park Bankwood Way Birstall West Yorkshire WF17 9TB T: +44 1924 284240 F: +44 113 257 9718 e-mail: hallm@sec-1.com	15 Feb of every year 15 May of every year 15 Aug of every year 15 Nov of every year

e) Acquirer's Details

The quarterly external scan report should be forwarded to the Acquirer.

Acquirer	Contact Details	Reports Issued?
Barclays Merchant Services	Julia Constantinos Payment Security Risk Manager Barclaycard Global Payment Acceptance Pillar K15.2 1234 Pavilion Drive Northampton NN4 7SG Telephone: +44 (0) 160 425 4042 Mobile: +44 (0) 777 554 1189 Fax: +44 (0) 160 425 4517 e-mail: pci.taskforce@barclaycard.co.uk	Yes

8.1.7 Internal and External Penetration Test

a) **TfGM** must conduct a penetration test of both internally and externally visible infrastructure at least annually, **and** following significant infrastructure changes, e.g. operating system upgrade or the addition of a web server or a sub-network to the to the CDE.

b) External penetration tests performed by **TfGM** shall be conducted in accordance with the current PCI DSS requirements (see Section 8).

c) Testing shall include at a minimum both an application- layer and a network-layer penetration test; noted vulnerabilities must be corrected and testing repeated until passing results are obtained.

d) Tests must be performed by a qualified internal resource or qualified external third party; organisational independence of the tester must be ensured.

e) Details of the qualified third party conducting Penetration Tests.

Organisation	Contact Details
Claranet Unit 1 Bankwood Way Birstall West Yorkshire WF17 9TB	Adam Hepworth Senior Account Manager Telephone: +44 (0) 1924 284 242 e-mail: AdamH@sec-1.com

8.1.8 Vulnerability Assessment Report

a) **TfGM** shall ensure a quarterly external report detailing all vulnerabilities and observations is produced following by an approved vendor (ASV) approved by PCI SSC.

b) This report shall be presented to the **TfGM Head of IS Operations** who shall disseminate the information to the relevant staff in order for any necessary remediation to occur.

c) Should the report highlight a serious issue, the person responsible for the network, host or software shall be informed immediately so that appropriate measures can be taken to either correct the issue or mitigate the risk of the issue being exploited until a permanent fix can be found.

8.1.9 Document in the Change Control System

All changes conducted after a Vulnerability Assessment shall be subject to internal change control procedures.

The Change Request form shall include references to the report detailing the issue it seeks to address before being rolled out.

8.1.10 PCI Assessment

The PCI On-Site Assessment shall be completed annually by the TfGM QSA as it forms an essential part of the compliance process.

8.2 Remote and Non-Physical Access Services

8.2.1 Remote Access to Services

a) **TfGM** shall ensure that all remote access technologies conform to the procedures in *Network, Applications and Systems Hardening* contained in this document.

b) **TfGM** shall utilise a two-factor authentication system wherever users need to access the CDE remotely via VPN (e.g Cryptocard).

8.2.2 Security of Third Party Access

a) Third party connections require additional scrutiny. The following statements will govern these connections:

   i) Connections to third parties must use a firewall or Access Control List (ACL) to separate the **TfGM** network from the third party's network.

   ii) Third parties will be provided only the minimum access necessary to perform the function requiring access. If possible this should include time-of-day restrictions to limit access to only the hours when such access is required.

   iii) Wherever possible, systems requiring third party access should be placed in a public network segment or demilitarized zone (DMZ) in order to protect internal network resources.

b) If a third party connection is deemed to be a serious security risk, the **Head of IS Operations** will have the authority to prohibit the connection.

c) If the connection is absolutely required for business functions, additional security measures should be taken at the discretion of the **Head of IS Operations**.

d) Third party access must be discussed with **IS Operations Team** prior to agreement being reached.

8.2.3 Restricting Third Party Access

a) Best practises for a third party connection require that the link be held to higher security standards than an inter-company connection. As such, the third party must agree to:

   i) Restrict access to **TfGM's** network to only those users that have a legitimate business need for access.

   ii) Provide **TfGM** with the names and any other requested information about individuals that will have access to the connection. **TfGM** reserves the right to approve or deny this access based on its risk assessment of the connection.

   iii) Supply **TfGM** with on-hours and off-hours contact information for the person or persons responsible for the connection.

   iv) If confidential data is involved, provide **TfGM** with the names and any other requested information about individuals that will have access to the confidential data. The steward or owner of the confidential data will have the right to approve or deny this access for any reason.

8.2.4 Third Parties Accessing Card Networks

a) None

8.2.5 Company-Owned Mobile Computing Devices

a) **TfGM** shall ensure that company owned devices connecting to the network have updated anti-virus software, personal firewall software activated and automatically updated and rules that cannot be modified by the user.

b) In the case of mobile / smartphone / tablet devices, anti-virus / malware protection / firewall software will be used where available.

c) The anti-virus and firewall software must have rules configured by TfGM that cannot be modified by the user. These rules must be specifically defined for mobile computing devices.

d) Applicable devices will be recorded using the F10 – Network Access using Mobile or Employee Owned PC's.

8.2.6 Mobile and Non-Company Owned Devices

It is expressly forbidden to connect mobile and non-company-owned (private) devices to the company network, and any non-compliance would be dealt with in accordance with **TfGM** disciplinary processes.

8.3 Network, Application and Systems Hardening

8.3.1 Principle Objectives

a) **TfGM** shall take all prudent steps to ensure that only users authorised to have access to its resources are able to do so.

b) **TfGM** shall ensure that all its electronic resources have access control systems in place to prevent unauthorised accounts.

c) **TfGM** shall ensure that all electronic resources dealing with credit card data require the use of secure authentication systems.

8.3.2 Accountability and Auditing

a) Asset Identification

Every device and the associated product, approved and used by **TfGM** will have an asset number and be clearly labelled **TfGM** so it it possible to determine the owner, contact information and purpose of each device.

Devices and systems include remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data / digital assistants (PDAs), e-mail and Internet usage.

The TfGM shall maintain an inventory with the asset number. Inventory shall be updated monthly.

The inventory will contain a list of all TfGM approved devices, associated product code and the personnel who are authorised to use such devices (where the devices are for end-user use).

b) Logs

- Logs must be include all security events from the following devices:
- for external-facing technologies (e.g. wireless, firewalls, DNS) onto a log server on the internal LAN.
- All system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and or SAD.
- All critical system components.
- All servers and system componement that perform security functions (for example, firewalls, intrusion detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc).

i) Wireless Logs

Ensure that audit trails are enabled and active for any wireless networks.

ii) Server Logs

Any server holding cardholder data must log the following:

- Actions taken by any individual with root or administrative privileges.
- Access to audit trails.
- Invalid logical access attempts.
- Use of Identification/Authentication methods.
- Initialisation of Audit Logs.
- Creation/Deletion of system-level objects.
- Elevation of privileges to root or administrative level.

iii) Application Logs

Each application that handles payment card data must log the following:

- All individual access to cardholder data.
- Actions taken by any individual with root or administrative privileges.
- Access to audit trails.
- Invalid logical access attempts.
- Use of Identification/Authentication methods.
- Initialisation of Audit Logs.

iv) Event Logs

For each event logged above, the following must be recorded:

- User Identification.
- Event Type.
- Date & Time.
- Success or Failure indication.
- Event Origination (e.g. IP address).
- Reference to the data, system component or resource affected.

c) Audit Trails

Ensure for all forms of audit trail above, that:

- Only users with a need-to-know can access audit trails, as defined in PR11 - Log Review Procedure.
- Audit trails are protected against unauthorised modification.
- Audit trails are backed up to a central log server, or to media that is difficult to modify.
- File integrity monitoring software is used to detect unauthorised modifications to critical system files, application executable files, configuration files, parameter files, content files, centrally stored, historical or archived audit or log files. Configure the software to generate alerts to perform critical file comparisons

at least weekly, and follow up unauthorised changes as defined in PR08 - Security Incident Management Procedure.

- Audit trails are reviewed at least daily by the **TfGM Serviceline**, with any erroneous entries being followed up. Reviews should be recorded as part of a daily check. See F18- Daily Security Checklist.
- Audit trails are kept (whether online or via restoring from backup) for at least a year, and can be restored as defined in PR11 - Log Review Procedure.

8.3.3 Time Synchronisation

a) In order to ensure that log times are accurate and events between systems can be accurately correlated, NTP (or similar) must be used on all critical systems.

b) In addition, the following configuration must be adhered to:

- Ensure that no more than two or three NTP appliances act as master time servers for the organisation. These master time servers shall obtain the time from an industry accepted external time source;
- Ensure that other servers synchronise only with **TfGM's** master NTP Appliances;
- The updates are encypted with a symmetric key and access control lists specify the IP addresses of client machines that will be provided with the time updates.
- Ensure that all critical systems have the correct and consistent time;
- Ensure that all NTP appliances are operating on the same and latest version;
- Ensure the external time source adhere to either International Atomic Time or Co-ordinated Universal Time (UTC);

- Ensure that the NTP appliances shall only accept time updates from the configured external source.

c) The **TfGM** NTP appliances shall obtain the time from an external source, Global Positioning System (GPS) synchronized with UTC (co-ordinated Universal Time).

d) Details on how the NTP is configured for all type of system components have been defined in the following System Hardening Guides:

- Firewall, Routers & switches Hardening Guide;
- PCs and Laptops Hardening Guide
- Server Hardening Guide.

8.3.4 Hardening Guides

a) System security parameters must be configured to prevent misuse by removing all unnecessary functionality.

b) **TfGM** must develop and maintain a Systems Hardening Guide for each class of system it deploys on the card processing network (for example, web servers, e-mail servers). These documents shall contain guidance on configuring the host to an industry-accepted security standard i.e. following SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS) guidelines).

c) In addition **TfGM** must use Cisco published documents, 200150 Cisco Guide to Harden Cisco ASA Firewalls and Cisco Infrastructure Device Access Checklist to develop the Hardening Guide for Cisco equipment used in the CDE.

d) Hardening Guides are as follows:

Document Name	Description	File Reference

Document Name	Description	File Reference
Firewall, Routers & switches Hardening Guide	Defines procedure related to measures taken to ensure the security and integrity of all firewalls, Routers and switches deployed in the TfGM CDE.	TfGM IS Hardware Hardening Guide.
PCs and Laptops Hardening Guide	Defines procedure related to measures taken to ensure the security and integrity of PCs and Laptops deployed in the TfGM CDE.	TfGM IS Hardware Hardening Guide.
Server Hardening Guide	Defines procedure related to measures taken to ensure the security and integrity of Access Control and Log Management servers deployed in the TfGM IS environment.	TfGM IS Hardware Hardening Guide.

e) **TfGM** must maintain a list of common security settings (group policies) for networked hosts and ensure that it is regularly updated and applied to previously-deployed servers.

f) Any modifications to any host shall trigger a review of the hardening guide to include the modification into the guide.

g) Application of a specific build standard should be recorded for future reference. See F11 – Build Standard Application Checklist.

h) Ensure **TfGM's IS DCS Team** is aware of common security settings for system components.

i) The system hardening guide will be updated as new vulnerabilities are identified thereby ensuring they address all known security vulnerabilities.

j) Systems Hardening Guides must include the following:

- The hardening guides must identify the functions provided and document how only one primary function is implemented per physical / virtual system.

- For any physical or virtual systems that cannot maintain a separation of duties, the **TfGM's IS DCS Team** shall record the justification for it and review the situation on a quarterly basis.
- All unnecessary and insecure services / daemons / protocols must be disabled on the host and these parameters must be listed, along with an explanation detailing why the services / daemons / protocols are disabled.
- A list of all necessary insecure services / daemons / protocols which must be enabled on the host and a justification included of why the service is enabled. Steps taken to implement the services / daemons / protocols securely need to be documented.
- All unnecessary functionality, e.g. software libraries, scripts, drivers, features, functions, files and unnecessary web servers must be removed, and an explanation provided of why they were removed.
- Administrator access to hosts (including access via web-based management interfaces) must use strong encryption (currently 128 bit or above). Examples include SSH on Linux / UNIX systems or network components and VPN Remote Desktop for Windows systems.
- All insecure remote access login commands must be disabled per host (e.g. telnet, rlogin).
- Details of default accounts to remove or disable when setting up equipment, software or associated technologies.
- All enabled security parameters need to be set appropriately and documented. Checks need to be carried out to determine if any functionality has not been documented and that only documented functionality is present on the system components installed.
- All use of encryption technology (wireless, VPN, remte access, authentication, data encryption) must be configured as secure and strong by default – it must not be possible for a user, administrator or end user to select a non-secure or weak setting.

k) In addition, all software and devices shall be set to ensure they comply with **TfGM's** Password management policy, see Section 8.4.3 and 8.4.4 of this document.

l) Access to any data storage system (including, but not limited to: Department or Group Filestore, E-Mail, or Databases shall require each user to authenticate with their username, password and use strong encryption (128 bit or above).

m) Permission to execute direct SQL queries shall be limited to Database Administrators only.

8.3.5 Dial-in or Remote Access Services

a) If remote access is permitted, **TfGM** must ensure that:

- Authorised remote-access sessions are automatically disconnected after a defined period of inactivity for 20 minutes.
- Remote-access is only activated for authorised vendors following receipt of an approved request, with immediate deactivation immediately after use.

8.3.6 Firewalls & Routers

a) Firewall & Router Setup/Configuration Standards

i) All machines with externally-facing IP addresses shall have a firewall configuration that only allows access to the services the machine is required to present to the outside world.

ii) The firewall shall perform a stateful inspection of all packets entering the network and only "established" connections (i.e, those originating from within the network) will be allowed on the network.

iii) All traffic shall be limited to the minimum necessary for the use of cardholder data.

iv) For each network component, **TfGM** shall maintain and document a list of IPs, ports, services, protocols and a description of groups, roles (including services) and person(s) responsible, See: F02 – Firewall Ports Required for Business.

v) Routers are subject to the same configuration stipulations and procedures as Firewalls.

vi) Routers/Firewalls shall be set to run in a secured configuration from boot up, all changes shall be saved to ensure they are not lost after reboots.

vii) **TfGM** shall ensure that configurations are synchronised between all routers.

viii) All firewall rules shall default to **DENY** for all inbound and outbound traffic.

ix) For each network component, **TfGM** shall maintain a list of ports required for business; refer F02 – Ports Required for Business.

x) A firewall needs to be in place between any DMZ and the internal network zone, further information supplied below.

xi) Firewall configuration documents can be found at:

Document Name	Description	File Reference
PR07 – IS Firewall & Router Security Procedure	Defines procedure related to measures taken to ensure the security and integrity of all firewalls and routers installations in the TfGM CDE.	PR07 – IS Firewall & Router Security Procedure

b) De-Militarised Zone

i) There shall be a segregated portion of the internal infrastructure designated to deal with all inbound facing requests, known as the DMZ.

ii) The DMZ shall be separated from the remainder of the internal network (including the CDE), and from the Internet by a firewall. This firewall shall only present the minimum number of ports required to allow the machine to perform its function. Traffic from external hosts to hosts on the DMZ shall be limited to those ports required for business purposes. Justification for

each open port must be recorded in line with firewall regulations.

iii) The firewall shall restrict all inbound traffic to only allow access to services on the machines within the DMZ. Internal addresses shall not be able to pass through the outside world into the DMZ.

iv) **TfGM** must restrict outbound traffic from the cardholder applications to within the DMZ only. Hosts on the DMZ shall only be able to pass data from themselves to other hosts on the network on prescribed channels. Firewalls shall be configured to only accept connections from a specified port on a specified IP.

v) Systems that handle or process cardholder data shall only be able to pass traffic to relevant hosts within the DMZ.

vi) Database servers shall be separated into their own internal DMZ, subject to standard DMZ rules. This internal zone shall not be routable from the public internet.

c) Internal Network Separation

i) The internal network (not including those machines deemed to be on the DMZ) shall be separated from the network by means of Network Address Translation.

ii) **TfGM** shall ensure that systems with a similar purpose are separated onto distinct subnets in accordance with RFC 1918, utilising VLAN or physically-distinct cabling.

iii) **TfGM** shall not use a randomly selected IP address range for its internal traffic.

iv) **TfGM** shall implement IP address masquerading to ensure that the private addressing scheme used internally is not leaked outside of the network.

v) Process for sending IP addresses

- **TfGM** shall classify the IP Addresses used in the CDE as Confidential. The IP addresses forwarded using e-mails to the internal staff and Service Providers to configure the AFC system and manage projects shall be on need to know basis and shall not be distributed widely.
- **TfGM** shall clearly instruct internal staff and Service Providers that:
    - IP Addresses associated with the CDE shall only be retained in secure storage in encrypted form;
    - all hard copies and any saved files shall be deleted when there is no business requirement to hold the information any longer all hard copies and any saved files shall be deleted.

d) Adding / Modifying Router Configurability and Firewall Rules

i) All changes made to network connections shall require a Change Request to be completed and approved by the **TfGM's Change Advisory Board.** The Change Request must contain the change required, the duration and the justification for the change. All changes made to the router need to be tested to ensure they achieve the desired effect and also do not cause other security issues.

ii) All changes made to the firewall shall require a Change Request to be completed and approved by the **TfGM's Change Advisory Board.** The Change Request must contain the change required, the duration and the justification for the change. All changes made to the router need to be tested to ensure they achieve the desired effect and also do not cause other security issues.

iii) All changes made to the router shall require a Change Request to be completed and approved by the **TfGM's Change Advisory Board.** The Change Request must contain the change required, the duration and the justification for the change. All changes made to the router need to be tested to ensure they achieve the desired effect and also do not cause other security issues.

e) Firewall Rule Justification

i) **TfGM** shall record the justification and requirements for each port/service on the firewall, especially *risky* services such as FTP / Telnet / POP3 / IMAP / SNMP etc or other services that do not use encryption during the storage, processing or transmission of cardholder data.

ii) This justification shall form the basis for reviewing if the firewall port is required. The justification shall also detail any mitigating steps taken to secure risky service (e.g. ACLs).

f) Review of Firewall Rules

i) Firewall rules placed on any of the network hosts shall be reviewed on a quarterly basis to ensure that the rules on the firewall are current and do not present a risk to the network integrity.

ii) The **TfGM Head of IS Operations** shall have a report prepared after each review, detailing the current firewall rules, and any changes made.

g) Network Segmentation

i) Where network segmentation is being used to reduce the scope of the cardholder data environment, then for each network segment, **TfGM** must document which segment(s) transmits cardholder data, and the mechanism by which segmentation is configured.

ii) The **TfGM Head of IS Operations** shall have a report prepared after each review, detailing the current firewall rules, and any changes made.

8.3.7 Network Diagram

a) **TfGM** shall ensure that a new network layout diagram is generated after any change to the network and that the diagram is circulated to all relevant parties.

b) The diagram shall document all connections to cardholder data (and clearly define wireless networks).

c) The network diagram should include both inbound and outbound card data flows, as well as transaction flows to acquirers.

d) The current diagram should be consistent with the firewall configuration standards.

e) The network diagram should be subject to version control and kept current. A documented process should be created describing how the network diagram is kept current.

8.3.8 New Equipment/Software Installation

a) System configuration standards shall be developed and applied when new systems are configured and verified as being in place before a system is installed on the network.

b) New equipment being installed on the network system shall be screened prior to installation for default usernames and/or passwords, SNMP community strings, web based administration interfaces and other remote configuration utilities.

- Default passwords shall be changed to comply with the **TfGM** password management policy, see Section 8.4.3 and 8.4.4 of this document.
- Where possible, configuration utilities shall be set to only accept connections from machines inside the trusted network. This shall be done through the use of access control lists or firewall restrictions.

c) The **IS Operations Team** shall ensure that:

- generic user IDs and accounts are removed from systems prior to deployment; and
- Group shared administration accounts are disabled for all network components.

8.3.9 Systems and Update Monitoring

a) Security Monitoring

i) The **IS Operations Team** shall monitor update lists for each vendor (Cisco and Microsoft) supplied components used in CDE network and in-scope servers, and resolve any issues brought to their attention by said list.

ii) The **IS Operations Team** will implement a process that assigns a risk ranking to newly discovered security vulnerabilities. Criteria should be used for ranking risk vulnerabilities identified, e.g. CVSS scores or high / medium / low categories.

iii) The **IS Operations Team** shall also monitor supplier security lists (such as Cisco Notification Service and Microsoft Security Bulletins) to maintain a thorough understanding and appreciation of on-going security threats both internally and externally. The **TfGM** system configuration standards must be reviewed and updated as new vulnerabilities are found.

iv) **TfGM** shall use the CVSS score published by Microsoft, Cisco, NESSUS and a reputable third party such as http://www.cvedetails.com .

b) Systems Updates

i) **TfGM** shall maintain a list (or have the capability to generate one) of patches installed on every server.

ii) Software updates shall be applied to internal systems on an on-going basis to ensure the systems are hardened against developing security threats.

iii) Software and security patches for critical infrastructure must be installed within 30 days of release and lower priority infrastructure within three months.

iv) Software updates to Production systems shall be scheduled to occur during non-operational hours prior to the commencement of the business day. This downtime shall be advertised beforehand in order to minimise disruption.

v) Updates destined for live systems shall be tested beforehand on test systems to determine whether or not they shall cause any disruption to front line, client facing systems.

vi) Should an update cause a piece of production software to fail during testing, then the patch vendor and the software vendor shall be contacted to ascertain where the error is occurring and how it should be resolved.

vii) All updates shall require the person completing the update to complete the Change Control entry and obtain sign-offs as detailed in PR05 - Change Control Procedure.

c) Anti-virus & Spyware

i) **TfGM** shall install and regularly update anti-virus software and spyware/malware detection software for periodic scans to detect, log and deal with such threats of all company machines with systems that may be affected. (see PR04 – Information System Anti-Virus Procedure)

ii) **TfGM** shall confirm anti-virus software and spyware / malware detection software is current, actively running and capable of generating audit logs.

iii) **TfGM** shall engage in weekly network scans to search for viruses on the entire network.

iv) The anti-virus software shall be configured so it cannot be disabled by regular users and logs virus removal from any hosts. Hosts found to be infected shall be removed from the network to prevent the spread of viruses to other hosts.

v) The **TfGM IS DCS Team** will take all appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the **TfGM IS DCS Team** may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

vi) Anti-virus servers must be configured to notify the **IS DCS Team** if a virus is detected on the **TfGM** network, and log the file, the user, the date and time, the IP address of the workstation and the virus ID. Anti-virus logs will be retained in accordance with PR02 - Log Retention Procedure.

vii) The **TfGM's IS Serviceline** will notify users of **TfGM** systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

viii) The **TfGM's IS DCS Team** will ensure that all risky file extensions are blocked by the e-mail / mail sweeper servers. Anti-virus software should be configured in accordance with PR04 – Information System Anti Virus Software Procedure.

8.4 User Account Management (Network & Application Level)

8.4.1 Issuing of Accounts

a) The users shall obtain explicit approval from the **TfGM Head of IS Operations** or the nominated deputy to use the systems (technologies)

b) The **Head of IS Operations** or the nominated deputy is responsible for ensuring that access is formally granted and that accounts are issued to users in accordance with PR03 - Logical Access Procedure.

c) Each employee shall be issued a unique user account and and a unique password, to access each system. The unique user account and and the unique password are for the individual's own use only.

d) The account must be configured to require the password to be changed immediately after first use.

e) Upon commencement of employment, the new user account shall be activated by the IS Team**,** and a password set in accordance with **TfGM** CDE password policy, (see Section 8.4.3 and 8.4.4 of this document), or issuing of token device or biometrics, as is relevant.

f) Under **no** circumstances shall group or shared accounts be issued to **any** user(s) even if requested.

g) If any group, generic or shared accounts are found they should be either disabled or removed.

h) The issuing of accounts must follow these guidelines for all critical technologies used to access the cardholder data environment, including remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data / digital assistants (PDAs), e-mail and Internet usage.

i) The **Head of IS Operations** or the nominated deputy is responsible for ensure that all access to cardholder data is controlled and monitored.

j) The creation of accounts is on the basis of the personnel's job classification and function.

8.4.2 Completion of Paperwork

a) The **TfGM's IS DCS Team** shall maintain a list of all users who have access to a given system and devices.

b) The **TfGM's IS DCS Team** shall ensure it is updated at least quarterly.

8.4.3 Changing/Resetting Passwords

a) All user ids are unique to each individual accessing the cardholder data network. All LAN user passwords shall:

   i) Be required to change every 90 days or less, and

   ii) Not be shorter than 14 characters,

iii) Contain a mixture of at least three out of the following character types:

- upper case alphabetical characters;
- lower case alphabetic characters;
- special characters;
- numbers;

iv) Cannot be the same as any of the user's 24 previous passwords; and

v) Cannot be any part of the user name.

8.4.4 Password/Session Lockout and Resetting

a) Password Lockout and Resetting

i) Applications and Network infrastructure shall lock access to an account after five (5) failed login attempts.

ii) Locked accounts shall remain locked on for 30 minutes.

iii) Unlocking/Resetting passwords during the locked in period shall require the user to contact the **TfGM's IS Serviceline** directly to verify the user is legitimate.

iv) The reset passwords must be set to a unique value for each user.

v) The reset password shall be changed after the must be changed after the first use.

b) Session Lockout and Resetting

i) Remote Login sessions shall time-out after being idle for 10 minutes and require the user to re-login.

ii) Local login sessions shall lock after 5 minutes to prevent unauthorised access to user data.

iii) The User shall be required to input his or her password in order to continue.

8.4.5 Vendor/Support User Accounts

a) User accounts issued to product vendors or for support purposes shall only be activated when required for support requirements, and disabled immediately when no longer required.

b) Vendor accounts for remote access should be monitored while being used, and access should be restricted to the time period needed in accordance with PR03 Logical Access Procedure.

8.4.6 Termination/Suspension of Account

a) Termination/Suspension of Employment

i) The **TfGM's IS Serviceline** shall be informed as soon as a person's employment is terminated without exception, and be required to suspend the former employee's access credentials immediately.

ii) Should a member of staff be suspended as a result of a disciplinary procedure, the **TfGM's IS Serviceline** should be informed and access to electronic resources shall be suspended immediately until the procedure is completed.

b) Inactive and Expired Accounts

i) Accounts that have not been accessed for more than six (6) weeks shall be considered Inactive and shall be locked to prevent access. In order for the account to be reactivated, the user affected shall be required to contact the **TfGM's IS Serviceline** directly.

ii) ***Inactive Accounts*** which are reactivated shall require the password to be changed.

iii) ***Inactive Accounts*** that have remained locked for more than ninety (90) days shall be considered ***Expired Accounts*** and shall be removed from the system.

8.5 Incident Response, Backup & Disaster Recovery

8.5.1 Backup Policy

a) All files considered essential for business continuity shall be backed up by the central backup system.

b) Credit Card Data and other Sensitive Information must be backed up in encrypted format to ensure sensitive information is stored and backed up securely.

8.5.2 Incident Response

a) **TfGM** shall have an incident response policy implemented to address the event of a security incident or compromise in the CDE.

b) The incident response policy, P03 - Disaster Recovery & Security Incident Response Policy, which must include the following:

i) Outline of roles and responsibilities, this must include 24/7 coverage for incident response and monitoring coverage.

ii) Communications Strategy.

iii) Coverage and responses for all critical systems and components.

iv) Procedures for notifying credit card associations and acquirers in the event of a compromise (or potential compromise) involving cardholder data.

v) Strategy for business continuity post compromise.

vi) References to card association incident response procedures.

vii) Analysis of legal requirements for reporting compromises.

viii) Periodic training of staff with nominated roles in P03 - Disaster Recovery & Security Incident Response Policy and PR08 - Security Incident Management Procedure.

c) **TfGM** shall ensure P03 - Disaster Recovery & Security Incident Response Policy is tested at least annually, with any deficiencies noted being corrected.

d) After resolution of an incident, review associated documentation from the incident and ensures that the correct procedures were followed.

8.6 Data Management (Access, Retention and Destruction)

8.6.1 Access to Cardholder Data

a) Automated access control systems will be implemented on all system components in the CDE.

b) Access to cardholder data shall default to deny-all and be granted on a need to know basis based on job function in accordance with PR03 - Logical Access Procedure.

c) Access control systems will have a default "deny-all" setting to ensure that users are given the minimum privilege access necessary in order to execute their job function.

d) Only users assigned to work as Database Administrators shall be given access to execute SQL queries directly.

8.6.2 Remote Access to Cardholder Data

a) Accessing cardholder data whilst connected via remote access from an external site is strictly forbidden, unless authorised by the **TfGM's Head of IS.**

b) The remote access technologies shall only be used to perform routine and/or emergency systems maintenance.

c) **TfGM** shall utilise a two-factor authentication system wherever users need to access the network remotely via VPN (e.g Cryptocard).

d) Copying, moving, or storing of cardholder data onto local hard drives or removable electronic media whilst accessing such data via remote-access technologies is strictly forbidden.

e) Access to Cardholder Data over wireless networks is not allowed, refer P04 - Wireless Access Policy.

8.6.3 Roles Access

a) **TfGM** shall maintain a list of each network host along with a list of which roles have access to that host.

b) **TfGM** shall maintain a list of each role and persons assigned to that role.

8.6.4 Transporting of Cardholder Data to outside bodies

a) Media needs to be classified to determine the sensitivity of the data.

b) **TfGM** shall maintain strict control over the internal handling, storage and destruction of any kind of media containing cardholder data (Confidential Data).

c) Any media containing cardholder data cannot be taken off-site.

d) **TfGM** shall ensure that if sensitive data (hardcopy or electronic media) needs to be sent offsite, it must be transported securely, e.g. by secure courier, and tracked so that safe receipt verified.

e) All information relating to the transport of media off-site shall be logged and retained for three (3) years.

8.6.5 Data Encryption

a) Sensitive data shall be stored in an encrypted format (where possible).

b) In cases where transfers are required of unencrypted data (e.g. to an acquirer), **TfGM** shall store the data unencrypted on an encrypted disk volume.

c) If this is not possible, **TfGM** shall store it on one server (subject to the tightest file system control available) for only as long as is necessary to perform the transfer (the data must then be subject to secure deletion procedures).

d) Details of how disk encryption is set up on the host system, and detail separation of encryption from native operating system controls.

8.6.6 Data Storage Restrictions

a) The following data shall not be stored by **TfGM** on any medium whatsoever under any circumstances unless otherwise specified:

- Track Data
- CAV2/CVC2/CVVC2/CID (Except for pre-authorisation transactions)
- Encrypted PIN block
- PIN or PIN Verification Values
- Full 16 digit card number (following authorisation)
- Full magnetic stripe data

b) For all instances where sensitive data is received and deleted as part of transaction processing:

- **TfGM** must Identify the document, defining the processes for securely deleting sensitive data.
- **TfGM** must verify the processes used to render data unrecoverable are tested and how sensitive data is confirmed as unrecoverable.

8.6.7 Data Storage Locations

a) Cardholder data is stored on the following locations:

- Customer Support Centre at 2 Piccadily Place;
- ESP Systex Ltd Mail Order Bureau Service Centre.

8.6.8 Data Retention

a) **TfGM** shall retain cardholder data for one of the following three purposes:

- Business
- Regulatory
- Legal

b) Cardholder data shall not be retained for longer than any retention periods defined in PR10 - Data Retention Procedure.

c) For data that is retained, the **TfGM's Management Accountant: Finance** must document what the data is, why it is being retained (Business, Legal or Regulatory reasons), which employees or group of employees shall have access and the date of the review.

d) At annual review, the **TfGM's Director of Finance and Corporate Services** shall review and document the justification for continuing the data retention.

e) Cardholder Data determined to have reached the defined retention period shall be subject to secure disposal, see P10 - Physical Security Policy, Section 8.3.4.

f) Records shall be kept of what has been destroyed, when, how and by whom. These records must not include any cardholder data.

8.7 Change Control

a) **TfGM** maintains a log of modifications made for the implementation of security patches and software modifications on any hosts on the network i.e.

- The person who made the modification.
- The date the modification was made.
- Who authorised the modification.
- What the modification entailed.
- The expected effect of the modification.
- The impact to the customer of the modification.
- Ensure functionality testing occurs before the change is implemented, to verify that the change does not adversely impact the security of the system.
- Ensure custom code changes comply with PCI DSS Requirement 8.5 before deployment into production.

- Ensure functionality testing occurs before the change is implemented, to verify that the change does not adversely impact the security of the system.
- Recovery procedures in case applied change does not have the desired effect or has an adverse effect.

b) Changes will be made in accordance with PR05 - Change Control Procedure.

8.8 Networked Equipment

a) **TfGM** shall ensure that all devices on the cardholder network are located within secure IS facilities.

b) **TfGM** shall ensure that all equipment on the network is sourced from a company approved products.

c) List of manufacturers for devices and systems used to access the cardholder network:

- Cisco for firewalls, routers and switches; and
- McAfee for IDS/IPS appliances.

8.9 Shared Hosting Provider

a) **TfGM** shall ensure that user processes running on a system with shared resources must use a unique user ID.

b) **TfGM** shall ensure that each entity's files must not be shared by group.

c) **TfGM** shall ensure that each customer's processes and CGI scripts are configured to run only as the customer's ID.

d) **TfGM** shall ensure that no entity on the system can use a shared web server user ID.

e) **TfGM** shall ensure that the user ID of any application process is not a privileged user (root/admin).

f) **TfGM** must restrict read, write, or execute permissions to files and directories an entity owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.)

g) **TfGM** must never issue privileged user accounts to its customers.

h) **TfGM** must restrict ownership of files and directories to specific entities.

i) **TfGM** shall ensure that customers do not write access to shared system binaries.

j) **TfGM** shall ensure that customers have only read access to its own audit trails.

k) **TfGM** shall ensure it has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.

l) **TfGM** shall ensure that hardware resources are protected against hardware's monopolizing in sub-systems such as:

- CPU;
- Memory;
- Network bandwidth;
- Disk Space.

m) **TfGM** shall ensure that for each customer:

- Logs are enabled for common third-party applications;
- Logs are active by default;
- Logs are available for review by the owning entity;
- Log locations are clearly communicated to the owning entity.
- Viewing of logs is restricted to the owning entity.

9 Glossary & References

9.1 Glossary – See Document P99

9.2 References

9.2.1 Policies

- P01 - IS Security Policy
- P02 – IS Security Audit Policy
- P03 – IS Disaster Recovery & Security Incident Response Policy
- P04 – IS Wireless Access Policy
- P10 – IS Physical Security Policy

9.2.2 Procedures

- PR02 - Log Retention Procedure.
- PR03 - Logical Access Procedure
- PR04 – Anti-Virus Procedure
- PR05 - Change Control Procedure
- PR08 - Security Incident Management Procedure
- PR11 - Log Review Procedure

9.2.3 Forms

- F04 - Change Control Form

Policy: P05 – IS Operational Policy				
Version	**Change**	**Reason for change**	**Date**	**Name**
2.0	Date and version	Updated policy	31/10/2013	C Burke
3.0	Date and version update	Updated annual policy	06/03/2014	C Burke
3.1	V2 to V3	Change variations	16/02/2015	C.Burke
4.0	Role names	Department rename	10/08/2015	J Singleton
4.1	Section 8.4.3	Changing/Resetting Passwords for 42 days to 90 days.	23/10/2015	C Burke
4.2	Date & Version	Annual Update	31/03/2016	C. Burke
4.3	8.6.7	Change of Address for Drivesafw	18/11/2016	C. Burke
4.4	8.4.1 & 8.4.4	Addition of unique Password	11/01/2017	C Burke
4.5	8.3.2 & 8.4.1	Reworded to meet the Requirement 12.3	12/01/2017	C Burke
4.6	8.3.4	Added Cisco hardening guide to meet Requirement 2.2	17/01/2017	C Burke
4.7	8.3.8 a) 8.4.1 i) 8.6.4	New Equipment Configuration Responsibility for Cotrol & Monitor of Cardholder Data Handling, Storage & Destruction of CHD	24/01/2017	C Burke
5.0	Date & Version	Annual Update – New Head of IS	31/03/2017	C. Burke
5.0	8.6.7	Removal of Drivesafe and Queens Road	13/03/2018	C. Burke
6.0	Annual Review	Change IS Infrastructure Manager to Head of IS. Removal of old firewall.	18/02/2019	C. Styler
7.0	Annual Review and Update	Change Head of IS to Head of IS Operations, IS team to IS Operational Team and IS Server Team to IS DCS Team.	25/03/2020	C. Styler

7.0	Annual Review	Policy now longer required – CDE no longer in scope	31/03/2021	C. Burke