Transport for Greater Manchester

Transport for Greater Manchester Policy

P03 IS Disaster Recovery & Security Incident Response Policy

Warning:

Printed copies of this document are uncontrolled
Check issue number on Intranet before using.

31/03/2021	31st March 2021	Document Reference no.	IS Disaster Recovery & Security Incident Response Policy P03
Version No.	8.2	Prepared by:	Catherine Burke
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 (Malcolm Lowe) 31st March 2021		Implementation date: 31st March 2021 Annual review date: 31st January 2022

Table of Contents

1 Policy Aims 3
2 Review and Update of the Policy Statement 3
3 Purpose 4
4 Scope 4
5 Policy Delivery 4
6 Accountability 5
7 Enforcement / Monitoring / Compliance 5
8 Policy 5
8.1 Disaster Recovery 5
8.2 Testing and Updating the Plan 8
8.3 Staff Training 9
8.4 Offsite Computing Facilities 9
9 Response Specific to Cardholder Data Security Incident / Compromise 10
9.1 Definition of a Security Incident / Compromise 10
9.2 Responsibilities of all Personnel 10
9.3 Compromise Coordination 11
9.4 Incident Response Plan 11
9.5 Contacting Other Parties 13
9.6 Forensic Investigation, ... 14
9.7 Ending the Response 14
9.8 Response to Media 15
9.9 Contacting End-Users 16
10 Glossary & References 17
10.1 Glossary 17
10.2 References 17

1 Policy Aims

a) This Disaster Recovery & Security Incident Response Policy Statement ("Policy Statement"):

   i) Sets out **TfGM's** Board high level requirements for the recovery of business assets in the event of a disaster situation. Specific attention is paid to the storage, processing or transmission of payment card data.

   ii) Defines the Incident Response statement for the business.

   iii) Applies to all payment card processing operations for the business and fraudulent use of credit cards.

b) In order to operate efficiently, **TfGM** has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients, customers and suppliers. Organisation that process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or to personal damage.

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 Team** to ensure:

   i) the business meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS).

   ii) it maintains its relevance to the business' current and planned Payment Card processing operations.

b) The **TfGM's Internal Audit Team** will keep an oversight of the annual review of the IS Disaster Recovery & Security Incident Response Policy.

3 Purpose

This document details the Disaster Recovery & Incident Response strategy for **TfGM** in relation to its network(s) that store, process or transmit payment card data. Its aim is to provide a detailed understanding of responsibilities for all levels of staff, contractors, partners and third parties that access **TfGM's** card data environment (CDE) in the event of serious network disruption.

4 Scope

a) This document should be reviewed by parties involved with **TfGM's** Payment Card processing operations. Specifically:

   i) Day-to-day (payment card processing) IS Operations.

   ii) Implementation of new (payment card processing) IS Systems.

   iii) Maintenance of existing (payment card processing) IS Systems.

   iv) Information Assets – includes both hard copy and electronic data and the hardware and software record keeping systems that support it.

   v) Information security incident – is indicated by a single series of unwanted or unexpected information security events and have significant probability of compromising business operations and threatening information security.

   vi) Security Breach – is an activity which causes or may cause the loss, damage or corruption of data.

b) This document should also be used for reference purposes when **TfGM's** undertakes its annual PCI compliance review.

5 Policy Delivery

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

6 Accountability

- **Responsonible to board:** IS Director
- **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

8.1 Disaster Recovery

8.1.1 Disaster Situation

a) A Disaster Situation in the context of this document is defined as an incident or combination of incidents that conspire to seriously impact on the business continuity of **TfGM**, automatic fare collection.

b) Occurance of (any) of the following will be considered a Disaster Situation:

i) Internet connectivity from Primary Data Centre

ii) Power Loss at Primary Site

iii) Fire or flood

iv) Data Security Breach (including loss or compromise of cardholder data)

v) Exclusion from business premises (e.g. due to snow/evacuation/bomb threat/pandemic)

c) The Incident Coordinator is responsible for ensuring that services are restored in a timely fashion.

8.1.2 Types of Incidents

a) A security incident, as it relates to **TfGM's** information assets, can take one or two forms. For the purposes of this policy a security incident is defined as one of the following:

   i) **Electronic**: This type of incident can range from an attacker or user accessing the network for unauthorised/malicious purposes, to a virus outbreak, to a suspected Trogan or malware infection.

   ii) **Physical**: A physical IS Security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain electronic information, and deliberate damage to any device or digital apparatus.

b) Electronic Incidents

When an electronic incident is suspected and reported to the **TfGM's Serviceline Practice**, **TfGM's** goal is to recover as quickly as possible, limit the damage done, and secure the network. The following actions must be taken as appropriate to the type of incident:

   i) Remove the compromised device from the network by unplugging or disabling the network connection. Do not power down the machine.

   ii) Disable the compromised account(s) as appropriate.

   iii) Report the incident to the Head of IS.

   iv) Backup all data and logs on the machine, or copy/image the machine to another system.

   v) Determine exactly what happened and the scope of the incident. Was it an accident? An attack? A Virus? Was confidential data involved? Was it limited to only the system in question or was it more widespread?

   vi) Provide an update to the Head of IS and management/executives as appropriate.

   vii) Contact the **InfoSec Practice**.

viii) Determine how the attacker gained access and disable this access.

ix) Rebuild the system, including a complete operating system reinstall.

x) Restore any needed data from the last known good backup and put the system back online

xi) Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.

xii) Perform Root Cause Analysis on the incident and determine measures that need to be put in place to ensure a repeat incident does not occur.

xiii) Review work instructions procedures and policies and make any amendments as required.

xiv) All security incidents must be reported immediately to the **Head of IS**.

8.1.3 Incident Response Guidelines

a) **TfGM's** Incident Coordinator and Security Incident Response Team provide 24/7 coverage for incident response and monitoring of systems.

b) Chain of command

i) In the event of a disaster situation, the order of succession shall apply to determine who has the overall command of the recovery.

ii) The **Incident Coordinator** will be the highest available person from the following list:

- **TfGM** Head of IS (Mobile: 07584 616689)
- **TfGM** Head of Operations (Mobile: 07741 833592)

c) Security Incident Response Team

The membership of **TfGM**'s Security Incident Response Team is defined in PR08 – Security Incident Management Procedure.

d) Containment / Coordination

i) In the event of a Disaster Situation, **TfGM** needs to quickly determine what has occurred and the best way to react.

ii) The **Incident Co-ordinator** should be alerted as soon as is practically possible in the event of such a disaster.

iii) Should the disaster involve (or is suspected to involve) a breach of data security procedures (e.g. external breach, leaking of cardholder data), the staff members immediately involved in the situation should take any steps they deem necessary to contain the security breach (including physical intervention, if necessary).

iv) In situations that do not involve a security breach or theft of cardholder data, the staff in attendance should take all necessary steps to restore service to a useable level.

e) Notification to Relevant Parties

i) Once the immediate disaster has been dealt with, **TfGM** needs to determine what has occurred and take one of two courses of action:

ii) In the event of a data security breach, **TfGM** needs to contact the acquiring bank/company to inform them of the incident. Once this has occurred, a Forensics Qualified Systems Auditor (FQSA) should be engaged and then respond to any recommendations made.

iii) Other situations, the **Security Incident Response Team** should formulate a plan to rectify the disaster situation, uncover details as regards to how the incident occurred and put in place suitable methods or procedures to minimise the risk of the situation occurring again.

8.2 Testing and Updating the Plan

a) **TfGM** will ensure that the Disaster Recovery plan is tested annually.

b) **TfGM** will engage in regular training sessions to ensure that staff are made fully aware of the implications of disaster situations on business continuity.

c) **TfGM** will regularly engage in testing data recovery from backup tapes to ensure data integrity and take appropriate action to correct the fault should data restoration fail.

d) **TfGM** will review and update the incident response plan, to take account of lessons learned and industry developments. As a minimum

Good Practice Guides for Security Incident Management published by the following organisations shall be checked for industry developments.

i) The National Cyber Security Centre
https://www.ncsc.gov.uk

ii) European Union Agency for Network and Information Security
https://www.enisa.europa.eu

iii) PCI Security Standard Council
https://www.pcisecuritystandards.org

8.3 Staff Training

a) All staff involved with business continuity will be made aware of P03 - Disaster Recovery & Security Incident Response Policy as soon as practically possible.

b) Staff will be aware of the significance of the data held on the systems and will have an appreciation of the risks should this data be lost or stolen

c) The **TfGM's Head of IS** will have responsibility to ensure that Staff are suitably trained to deal with disaster situations.

8.4 Offsite Computing Facilities

TfGM will maintain a list of all offsite or backup computing facilities, along with the address and contact details for the key-holders, including their role in the Security Incident Response Team.

Location	Keyholder(s)	Keyholder Phone Number	Keyholder Role	Status	Address
TfGM Office Helmet Street	Serviceline	0778 927 8609	Serviceline Engineer	Active	TfGM Helmet Street, Manchester M1 2NT
S & B	Chris Hart	07825 798833	Service Delivery Manager	Active	S&B Breite Strasse 41238 Monchengladbach Germany

9 Response Specific to Cardholder Data Security Incident / Compromise

9.1 Definition of a Security Incident / Compromise

a) A Security Incident / Compromise is defined as any of the following occurring and being detected in the cardholder data environment:

i) loss or theft of payment card data, especially the PAN (payment card number);

ii) loss or theft of secret keys used for encrypting payment card data;

iii) any evidence of unauthorized activity, such as entry into a **TfGM** equipment room on 3rd Floor, 2 Piccadilly Place;

iv) detection of unauthorized wireless access points;

v) critical IDS alerts;

vi) alert and/or reports of unauthorized critical system or content file changes;

vii) any evidence of **TfGM** staff sending or receiving full PAN through electronic media, such as e-mail, facsimile, text and etc.

9.2 Responsibilities of all Personnel

a) **TfGM** takes all possible steps, compliant with the PCI Data Security Standard, to ensure that a compromise should never occur. The likelihood of a compromise is therefore remote. However, **TfGM** is obliged to have a policy in place, regarding a Security breach or compromise and all personnel are obliged to follow this policy.

b) For the purposes of a compromise, all personnel includes all permanent and temporary employees of **TfGM** AND any sub-contractors of **TfGM** who have access to 'in scope' servers AND any employees of companies to which **TfGM** has out-sourced operations that relate to payment card data or 'in-scope servers, e.g. outsourcing of system administration.

c) All personnel, as defined above, must read, understand and annually sign this document, on commencing their work for **TfGM.**

d) The person detecting the compromise shall immediately note the server on which the compromise was detected, and the time, and

immediately inform the **Incident Coordinator** (see Section 8.1, Incident Response Guidelines).

e) If the compromise occurs outside normal business hours, an **Incident Coordinator** should be contacted using their emergency contact details, refer paragrapgh 8.1.3 a).

9.3 Compromise Coordination

a) As soon as the **Incident Coordinator** becomes aware of the compromise he shall assume responsibility for performing the Response Plan (see Section 9.4).

b) The **Incident Coordinator** can delegate all or part of the Response Plan to other personnel, but shall ensure that he is easily contactable throughout the period of the Compromise Response, as they are ultimately responsible for ensuring that the Response Plan is followed and all actions completed.

9.4 Incident Response Plan

a) The following describes the actions that should be followed, once an **Incident Coordinator** has become responsible for a Compromise Response.

b) A Compromise Response Log will be kept in paper or electronic format, details to be recorded are as follows:

i) The name and contact details of the person identifying the compromise.

ii) The file location for the Compromise Response Log.

iii) The time and location the compromise was detected, and

iv) The name of the **Incident Coordinator** and the time at which he became aware of the Compromise.

c) **TfGM's IS Team** member shall immediately work on containing the compromise and shall attempt to:

i) Prevent further (or any) loss of payment card data. This is more important than determining who or what caused the compromise, determining how the compromise occurred, or resuming normal operations. For example, should the System Adninistrator determine that the only way to

prevent data loss is to disconnect a server (or servers) from the network, then this should be done, even if it means that it will no longer be possible to determine how the compromise occurred.

ii) Determine who or what was responsible for the compromise (e,g, name or location of hacker, automated attack, etc);

iii) Secure the 'in-scope' system of **TfGM** against further compromise;

iv) Determine if any payment card data has been stolen, and if so, which data (list of cards);

v) Keep the **Incident Coordinator** apprised of the situation and actions being performed;

vi) Resume normal operations, once authorised by the **Incident Coordinator;**

vii) Log all actions performed and all information obtained regarding the compromise, in the Compromise Response Log.

d) The **Incident Coordinator** shall notify all personnel and other relevant parties, working during the period of the Compromise Response, that a Compromise Response is being followed, as soon as reasonably possible, and that normal operations will not be possible until notified later, see section 9.5 – 'Contacting Other Parties'.

e) Once the compromise has been contained, if any payment card data has been lost or stolen, a list of all affected cards shall be added to the Compromise Response Log. If the extent of the loss of payment card data cannot be determined, the 'worse-case' expectation of what data has been lost, shall be noted in the Compromise Response log. For example, this could be "PAN" an expiry data for all payment cards of all active end-users.

f) If Visa or Mastercard:

i) Specify that any actions be taken, the **Incident Coordinator** shall ensure that these actions are taken and logged in the Compromise Response Log. The **Incident Coordinator** shall also furnish Visa / Mastercard with any details or information regarding the Compromise, that they demand.

ii) Require that an external Forensic Team investigate the Compromise, the **Incident Coordinator** shall facilitate this.

g) If Visa / mastercard or an external Forensics Team appointed by either of them, suggest that legal action is taken in regard to the Compromise , then the **Incident Coordinator** shall assist in this legal action, as far as reasonably possible. The **Incident Coordinator** shall assist in any legal action, even if it is against any current or ex personnel of **TfGM** or any of the sub-contractors or outsourcing companies used by **TfGM**.

h) If it is determined that the compromise occurred as a result of the following, then they must be addressed immediately:

i) A'root-kit' has been or might have been installed on any 'in-scope' servers, then all passwords of all users must be changed.

ii) A weakness or bug in the application for which a patch is outstanding.

iii) Any secret keys used for encrypting payment card data have been or might have been lost of stolen, but the payment card data itself has not been stolen, then the affected payment card data shall be re-encryped accordingly.

9.5 Contacting Other Parties

The **Incident Coordinator** shall inform the relevant staff, Card Payment Brand owners, and other stakeholders of the compromise, including the following, as soon as reasonably possible.

a) All bank(s) Barclays Merchant Services with which **TfGM** has a Merchant Accounts

Acquirer	Contact Name	Contact Number
Barclays Merchant Service	Ian Gallier	07788 358 977

b) The Scheme owners, such as Visa, Mastercard etc will be contacted through the **TfGM** Acquirer Barclays Merchant Services.

c) All Service Providers (payment processors) 'downstream' of **TfGM**.

Service Provider	Contact Name	Contact Number
PayPoint	Stewart Jacobsen	07557 204483

Barclaycard PDQ	Ian Gallier	07788 358 977
Barclaycard SmartPay	Ian Gallier	07788 358 977
S & B	Chris Hart	07825 798833

The CEO and Directors of TfGM

Contact Name	Position	Contact Number
Bob Morris	Chief Operating Officer	0161 244 1022
Steve Warrener	Director of Finance and Corporate Services	0161 244 1025

d) The **TfGM** Head of Communications and Customer Services responsible for communicating with the Media.

Contact Name	Contact Number
Daniel McMullan	0161 244 0808

e) The TfGM's QSA Sec-1 Ltd

Contact Name	Contact Number
Wayne Murphy	01924 284 240

9.6 Forensic Investigation,

a) Further to any compromise, it may be necessary to facilitate a forensic investigation.

b) The forensic team will be selected by Visa Europe (or another card brand) and will require physical as well as network access to the compromised infrastructure.

c) **TfGM** will comply with all requests from the forensic investigators to access any compromised system.

9.7 Ending the Response

a) Once the **Incident Coordinator** is satisfied that all of the conditions below have been satisfied, then he can declare the end of the Compromise Response. The time, at which the Compromise Response is declared ended, shall be noted in the Compromise Response Log.

b) The Compromise Response shall not deemed to have ended until:

i) The system has been secured against further Compromise, and

ii) It has been determined how the Compromise occurred, and the extent of any payment card data loss, as far as reasonably practical

iii) The required patch or patches have been added to the application (if the application needs to be patched because a weakness or bug in the application was the cause of the Compromise).

iv) Password changes have been made, if required, as a response to the Compromise.

v) Re-encryption of payment card data has been completed, if required, as a response to the Compromise.

vi) Written authorisation is obtained from Card Payment Brand owners, if required, following a Compromise. In this case, the written authorization shall be appended to the Compromise Response Log and the time at which such authorization was obtained, shall also be noted in the Compromise Response Log.

c) Once the Compromise Response has ended, the **Incident Coordinator**:

i) Shall authorise a network security co-ordinator to resume normal operations, and

ii) Shall inform all personnel and all other parties who were informed of the Compromise.

9.8 Response to Media

a) There is a clearly defined process for dealing with the media and public relations during a Compromise, and it has been verified during tests. In the event of a Compromise, no approach shall be made to the Media. For the purposes of a Compromise the 'Media' includes (but is not limited to):

i) any written or printed newspapers, periodicals or trade publications.

ii) any radio or television stations.

iii) any internet based publications, such as web-logs, online periodicals.

iv) Any updates to social media channels such as Facebook / Twitter / LinkedIn.

b) If the Media contacts any personnel of **TfGM** then they must inform the **Incident Coordinator**. If deemed appropriate by the CEO, they can authorize the Marketing Manager of **TfGM** to release a statement to the Media making the enquiry.

c) The form of the Media release should be based on the suggested template shown below (amended as necessary, or as advised by **TfGM's** legal advisor):

"On [date] ***TfGM*** *determined that a compromise of customer data had occured.* ***TfGM*** has identified the cause of the breach, and has put measures in place to contain it, and to prevent it from happening again. All customer payment card data is maintained within **TfGM** in strongly encrypted form, in line with industry requirements, so at this time, it is believed that it is extremely unlikely that any sensitive payment card data was stolen in a usable form. Any payment card holders that might have been affected by this event will be informed accordingly.

TfGM *followed these procedures, to contain the Compromise. All sensitive payment card data is only maintained within* ***TfGM*** *in an encrypted form. It is believed that it is extremely unlikely that any sensitive payment card data was stolen in a usable form. It has been determined that data pertaining to your payment card may have been amongst the data stolen. You should inform the issuer of your credit card of this occurrence and request that the credit card is cancelled and a replacement issued."*

9.9 Contacting End-Users

If it is believed that payment card data may have been stolen/lost, as a result of the Compromise, then the Incident Coordinator shall inform all end-users that could have been affected, where possible.

End users shall be informed by e-mail to their registered e-mail address.

The form of the e-mail to end users should be based on the suggested template shown above amend as necessary, or as advised by the **TfGM** legal advisor.

10 Glossary & References

10.1 Glossary

See document P99 - Glossary

10.2 References

- PR08 – Security Incident Management Procedure

Policy: IS Disaster Recovery and Security Incident Response				
Version	**Change**	**Reason for change**	**Date**	**Name**
2.0	Date	Review and Update	30/10/2013	C.Burke
3.0	Date and Version	Annual Review	06/03/2014	C. Burke
3.0	Update	Updated to include Version 3.0 change variations	16/02/2015	C.Burke
3.1	Date and Version	Annual Review	31/03/2016	C Burke
4.0	QSA Details	New QSA	14/11/2016	C Burke
5.0	8.1.3 a)	Updated to include 24x7 cover	24/11/2017	C Burke
6.0	8.2 d)	Updated to include reference organisations to check Industry Developments	26/11/2017	C Burke
6.1	Date & Version	Annual Review, new Head of IS	31/03/2017	C. Burke
7.0	Annual Review	Annual Review	31/03/2018	C. Styler
8.0	Annual Review	Removal of Jon Lamont (CEO)	11/03/2019	C. Burke
8.1	Annual Review	Add Head of Operations	31/03/2020	C Burke
8.2	Annual Review	Pandemic, Team Name Change	31/03/2021	C Burke