Transport for Greater Manchester

Transport for Greater Manchester Policy

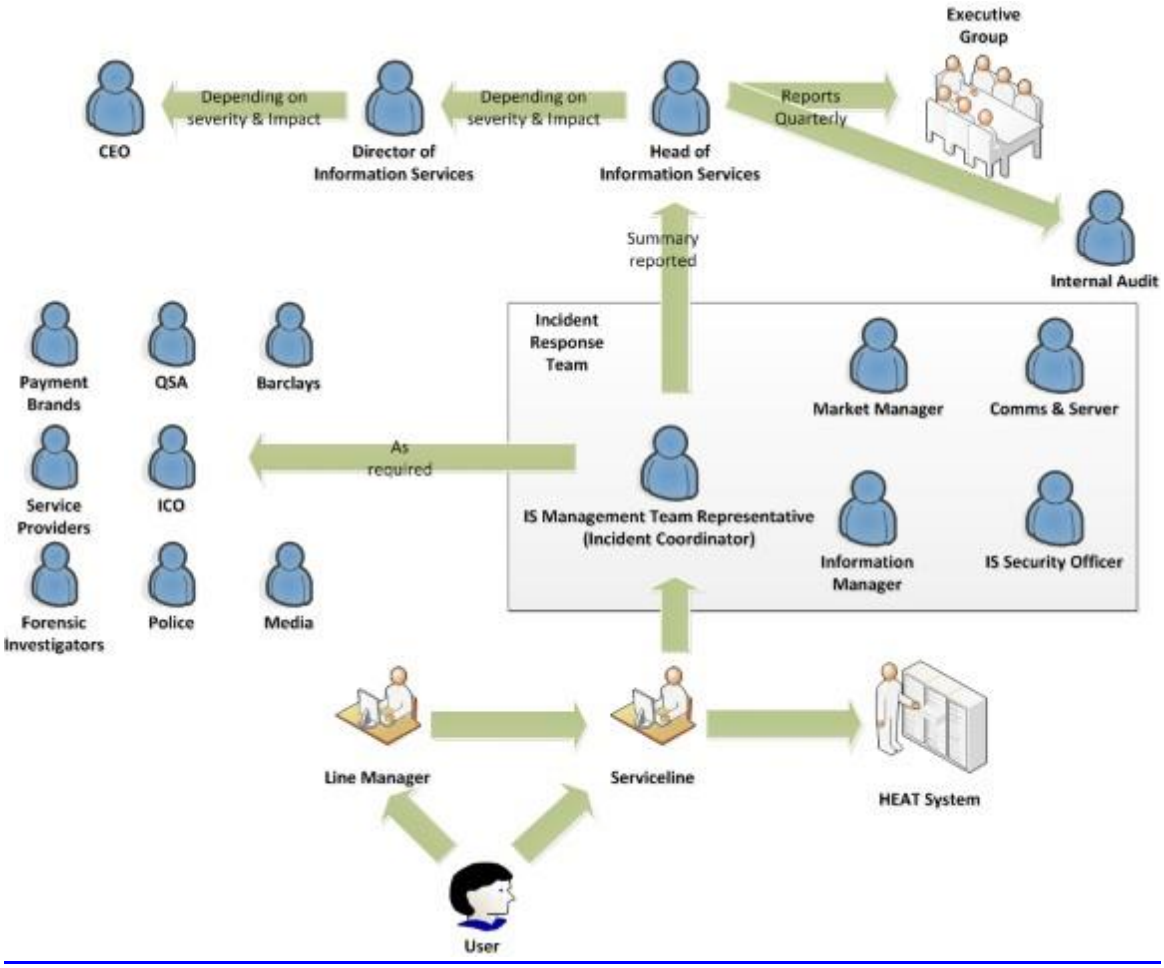
Security Incident Response Plan

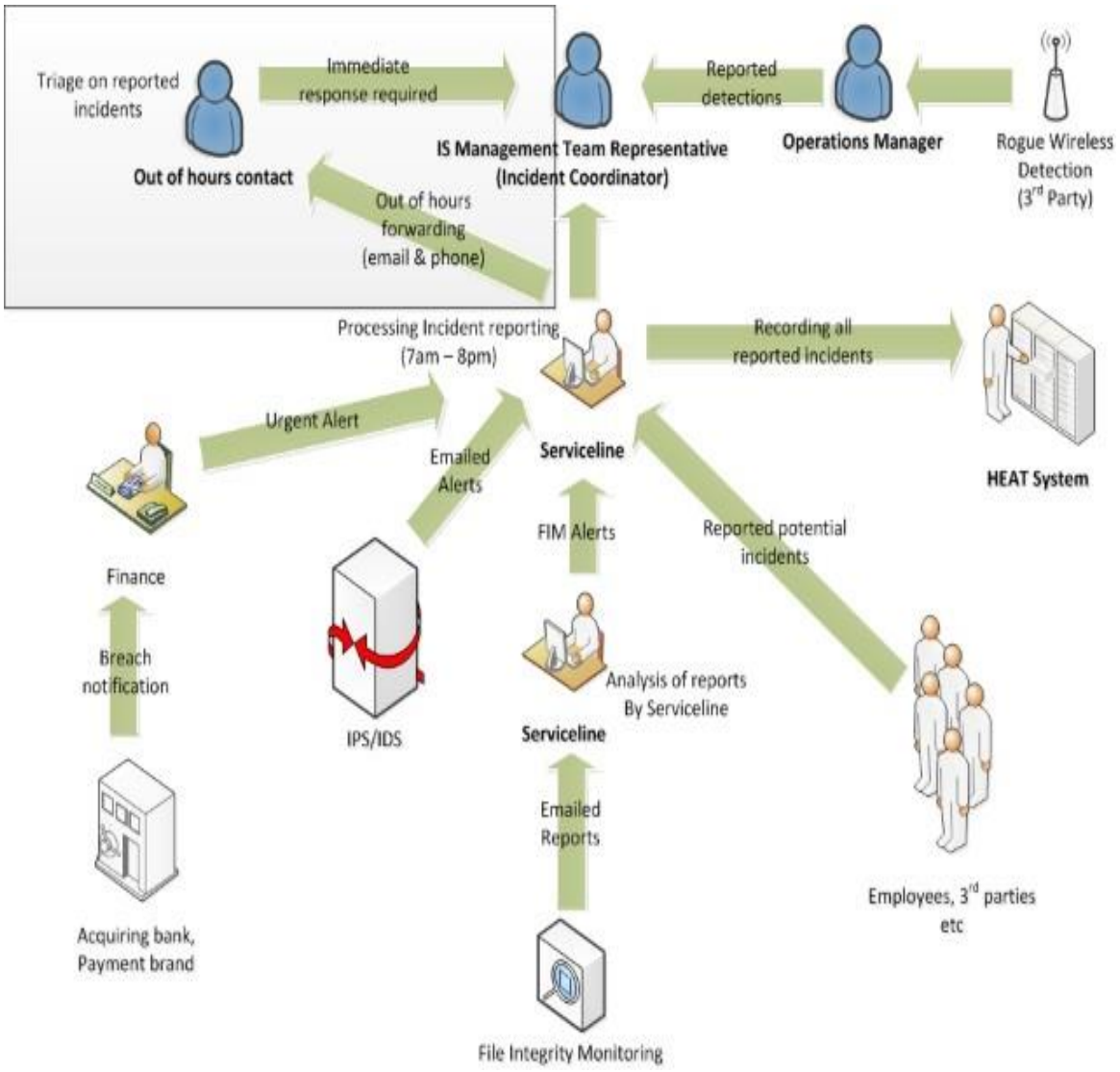
Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31st March 2021	Document Reference no.	Security Incident Response Plan
Version No.	8.0	Prepared by:	IS Management Catherine Burke
Equality Impact Assessment	Validation of Initial Screening Equality Officer: Muhammad Karim		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)		Implementation date: 31st March 2021 Annual review date: 31st January 2022


Executive Group
CEO
Depending on severity & Impact
Director of Information Services
Depending on severity & Impact
Head of Information Services
Reports Quarterly
Internal Audit
Summary reported
Incident Response Team
Market Manager
Comms & Server
Payment Brands
QSA
Barclays
As required
Service Providers
ICO
IS Management Team Representative (Incident Coordinator)
Information Manager
IS Security Officer
Forensic Investigators
Police
Media
Line Manager
Serviceline
HEAT System
User


Triage on reported incidents
Immediate response required
Out of hours contact
IS Management Team Representative (Incident Coordinator)
Reported detections
Operations Manager
Rogue Wireless Detection (3rd Party)
Out of hours forwarding (email & phone)
Processing Incident reporting (7am – 8pm)
Recording all reported incidents
HEAT System
Urgent Alert
Emailed Alerts
Serviceline
FIM Alerts
Reported potential incidents
Finance
Breach notification
IPS/IDS
Analysis of reports By Serviceline
Serviceline
Emailed Reports
Employees, 3rd parties etc
Acquiring bank, Payment brand
File Integrity Monitoring

1 Policy

a) In order to comply with the Data Security Standards of the Payment Card Industry, Transport for Greater Manchester, as an organisational entity, is required to operate, maintain, test and review a Security Incident Response Plan.

b) The Security Incident Response Plan is required to provide clear, concise instruction to respond immediately to a perceived breach; a potential breach or an actual breach of the of the cardholder data environment, including, but not limited to, the defined Cardholder Data Environment and the systems that affect the security of that environment.

c) In the context of this Security Incident Response Plan, a 'breach', also refers to Intrusion attempts, security breaches, other technical or physical security incidents perpetrated against **TfGM** owned computing or networked resources. As such an occurrence may jeopardise or compromise information assets, information systems or the network infrastructure of the organisation, it must be reported in accordance with this process defined in this plan.

d) This Security Incident Response plan is not restricted to Information Technology or the IS function. The contents of this plan encompass all relevant aspects of Information Security, including people, processes, technology, technological and physical security, the Card Holder Data Environment and apply equally to all **TfGM** employees and related activities.

e) The objectives of the Incident Response Plan are:

- To ensure all security incidents are reported and recorded;
- That all security incidents are investigated;
- That identified security incidents are considered within the Risk Assessment Process;
- That the impact of a security incident is minimised;
- That suitable action is undertaken to address and resolve the security incident;
- That suitable notification and reporting is completed;
- That a security incident is reviewed to provide 'lessons learned'
- That a security incident is analysed and measures taken to prevent reoccurrence are introduced, ie Control improvement

f) The Incident Response Plan sets out:

- Roles and Responsibilities;
- Specific contacts within the Incident Response Team;
- Reporting and Communications Strategies;

- Specific contacts for Escalation and Notification
- Classification of Security Incidents;
- Incident Response Procedures;
- Security Incident Reporting;
- Incident Response Plan Annual testing procedure;
- Incident Response Plan revision procedure;
- Business Continuity Implications;
- Legal Implications
- Audit Review

a) Annual Reviews

On an annual basis, the Lead Security & Compliance Analyst meets with customer representatives, where operational activities have been identified to link to card holder data or the card holder data environment, which could include access to; impact on; direct or indirect handling, maintenance or manipulation of card holder data. The meetings are structured to discuss potential risks and operational procedures, with supporting documentation produced.

b) Card Holder Data Environment (CDE)

Refers to the IT environment, which is used to store, transmit or access card holder data. This environment includes terminal equipment; network equipment, media and services; hosted servers; storage infrastructure.

c) Customer / Departmental Representatives

Refers to internal **TfGM** staff, representing Departments, Service Areas and Operational Units, as customers receiving professional IT services, either directly or indirectly, from **TfGM** IS.

d) Risk Assessment

Annual Risk Assessments are conducted by IS staff, specifically the Lead Security & Compliance Analyst, and representatives of service areas responsible for the receipt, handling and processing of card payments and card holder data. The risk assessments review operational processes and procedures and review known risk within physical environments, to ensure reasonable and realistic measures are maintained to protect the integrity of sensitive data.

e) Security Incident

Refers to potential, perceived or actual intrusion attempts, security breaches, or other technical security incidents perpetrated against **TfGM** owned computing or networked resources.

f) Service Provider

Refers to external contractors, individuals, organisations, or companies engaged to provide goods or services to **TfGM**.

2 Scope

2.1 The scope of this Security Incident Response Plan is referenced within 'The IS Disaster Recovery & Security Incident Response Policy PO3' and 'The Security Incident Management Procedure PR08', which is maintained as internal IS documents within the PCI SharePoint site.

2.2 The scope of the Security Incident Response Plan is limited to addressing the technical aspects of a perceived, potential or actual breach. The communications aspects that may arise from a breach are the responsibility of areas of the business outside Information Services. The Head of Information Services will act as liaison between the Security Incident Response Team and the administrative controls of the business, including for example, but not limited to Financial Services, Customer Services and Communications Services.

2.3 The Security Incident Response Plan applies to Transport for Greater Manchester (**TfGM**), as an organisational entity and includes all **TfGM** employees; **TfGM** Directorates; **TfGM** Operational Units; Service Providers; contractors; partners and any other third parties who may have access to the 'Card Holder Data Environment' (CDE).

2.4 It is everyone's responsibility to identify and report Security Incidents.

2.5 It is the responsibility of **TfGM** IS staff to ensure the Security Incident Response Plan is applied to address an identified perceived, potential or actual breach.

2.6 The scope of this Incident Response Plan will supersede any fault reporting procedures which may have been invoked prior to the identification of a perceived, potential or actual breach.

2.7 The scope of this Incident Response Plan will define the activities of IS Staff during a potential breach; a perceived breach or an actual breach.

2.8 A Security Incident can be an electronic or physical event which threatens; increases the risk to or compromises the card holder environment, equipment, infrastructure or data. All Security Incidents are to be reported in accordance with this Incident Response Plan.

3 Roles and Responsibilities

3.1 The roles and responsibilities for members of the Incident Response Team are contained within the 'Security Incident Management Procedure PR08'. In the context of this Incident Response Plan, the roles and responsibilities are summarised as follows:

3.2 All **TfGM** employees, Service Providers, contractors, partners and other third parties.

3.3 The continued operation of a secure payments system is critical to the operation of the organisation and as such it is essential that all persons involved at any level remain vigilant and act in a sensible and responsible manner. Anyone who identifies a suspicious event, no matter how minor, is required to take positive action and advise their line manager.

3.4 All **TfGM** employees, Service Providers, contractors, partners and other third parties should:

3.5 Watch for signs of security incidents and report any irregularities or suspicious activity immediately according to the instructions in this document.

3.6 Familiarise themselves with this plan and ensure they maintain access to the current version.

3.7 Maintain access to a current version of the **TfGM** contact list, contained within Section 4 of this document 'Incident Response Team'.

3.8 Quickly notify the appropriate parties of any incident as soon as it is detected and follow the instructions in this document for each type of incident.

3.9 Record a description of the incident as soon as it is reasonable to do so, and include as much detail as possible. Dates, times and actions should be documented in a 'Security Incident Response Report', refer to Appendix 1.

3.10 Immediately, contact Information Services for assistance to investigate the incident.

3.11 Refrain from reporting or discussing the incident with others except members of the 'Incident Response Team' identified in section 10 of this plan

4 Serviceline

4.1 The Serviceline function is the initial point of contact for reporting Security Incidents during normal working hours.

Serviceline will:

4.2 Ensure Incidents are recorded in the Information Services reporting system;

4.3 Provide initial advice of how to deal with a Security Incident to a caller;

4.4 Ensure that the Security Incident is immediately passed to the Lead Security & Compliance Analyst or escalated to the IS Management Team Representative.

4.5 Monitor systems and services for security incident alerts and respond to File Integrity Monitoring, Intrusion Detection and Intrusion Protection and rogue wireless device alerts by investigating and where necessary escalating detected alerts to IS Server and Network support staff.

4.6 Maintain relevant details of alert monitoring, escalation and corrective action, within the IS Knowledge Base, with specific reference to File Integrity Monitoring, Intrusion Detection and Intrusion Protection and rogue wireless device alerts.

5 Lead Security & Compliance Analyst

5.1 The Lead Security & Compliance Analyst will be available to devote efforts to resolving identified Security Incidents.

5.2 The Lead Security & Compliance Analyst will attend the Risk Assessment meetings, with customer representatives and will contribute to annual reviews.

5.3 The Lead Security & Compliance Analyst is formally trained to the CISSP standard and is considered to be competent to provide expert recommendation to maintain and enhance the security of **TfGM**, the associated networks and the card holder data environment; to safeguard evidence in the event of a Security Incident; and to manage investigative forensic work.

5.4 The Lead Security & Compliance Analyst will liaise with Serviceline and the departmental representatives to confirm an incident and to investigate the implications of any incidents.

5.5 The Lead Security & Compliance Analyst will coordinate documentation of the incident.

5.6 The Lead Security & Compliance Analyst will maintain active reporting to the IS Management Team representative.

5.7 The Lead Security & Compliance Analyst will analyse any security incidents and will suggest measures for an immediate, interim resolution or containment.

6 IS Management Team Representative

6.1 The IS Management Team Representative will be available to co-ordinate the resources required by the Incident Response Team and will manage the IS resources, with regard to the incident response.

6.2 The IS Management Team Representative will provide appropriate levels of reporting to the Head of IS, as to the progress and content of the Security Incident Response plan, and will deputise in his/her absence.

6.3 The IS Management Team Representative will ensure that the Lead Security & Compliance Analyst is fully available to deal with a reported Security Incident and is not interrupted by any other activities.

6.4 Any one of the IS Managers, including IS Head of IS Operations; IS Service Manager; IS Information and IS Business and Applications Manager, will be available to act as IS Management Team Representative.

6.5 An IS Management Team Representative will attend the Risk Assessments meetings, with customer representatives and will ensure annual Risk Assessment reviews are conducted.

6.6 An IS Management Team Representative will coordinate the 'Lessons Learned', 'Incident Response Plan Test Procedure' and 'Incident Response Plan Revision' activities.

6.7 The IS Management Team Representative will ensure that all activities are formally documented and reported, including all recommendations to prevent reoccurrence.

7 Data Protection Officer

7.1 The Data Protection Officer, will ensure that members of the Incident Response Team refer to, and comply with relevant policies, most specifically, the Data Protection Policy.

7.2 The Data Protection Officer, will consult with members of the Incident Response Team and advise the Head of IS whether the security incident should be notified to the Information Commissioners' Office.

8 Head of Information Services

8.1 Holds overall responsibility for technical aspects of the Security Incident Plan, but with authority to delegate any elements to other Information Services staff.

8.2 In the event of contested, conflicting or difficult issues, and/or where satisfactory progression toward resolution is not being made, the Head of Information Services has delegated authority to assume control of any Incident.

8.3 Responsibility to maintain the Incident Response Plan and to ensure that relevant technical activities, defined herein, are undertaken in a timely and responsive manner.

8.4 To maintain the operational integrity of the Incident Response Plan by ensuring completion of relevant test and revision schedules.

8.5 Where a security incident is identified, the Head of Information Services will ensure effective communication is maintained between all persons, which could include the technical activities of Information Services; associated partners; supplier organisations and the administrative function of the business.

8.6 Where a security incident is identified, the Head of Information Services will, after due consideration and consultation with the Lead Security & Compliance Analyst and the IS Management Team Representative, form an Incident Response Team. The Head of Information Services will have delegated authority to determine the structure, composition and membership of the Incident Response Team, including both internal **TfGM** resources and external organisations, as indicated within Section 10.

8.7 Where a security incident is identified, as a potential breach; a perceived breach or an actual breach, the responsibility for coordination and resolution is to be clear and uncontested. In these instances, overall control will be delegated to the Head of Information Services.

9 Internal Audit

The appointed Internal Audit representative will:

9.1 Be notified by the Lead Security & Compliance Analyst of each reported incident and the salient details;

9.2 Assess the likely risk of exposure to **TfGM**;

9.3 Determine the extent of Internal Audit involvement in subsequent investigations by the Lead Security & Compliance Analyst;

9.4 Receive the draft report on the outcome of investigation; and, if appropriate, contribute to the development of remedial (control improvement) actions;

9.5 Receive the final report into the incident and take steps to report to **TfGM** Audit Committee;

9.6 Determine the extent of any follow up audit review to confirm the effectiveness of action taken.

10 Incident Response Team

10.1 It is anticipated that the Incident Response Team will normally comprise internal **TfGM** resource. However, when an incident is considered to be sufficiently serious or critical, the Head of Information Services will have the delegated authority to liaise with, advise and co-opt the services of external organisations.

Internal contacts:	Name	Contact Number	E-mail / Address
Service Line		0161 244 1234	serviceline@tfgm.com
Lead Security & Compliance Analyst(s)	Catherine Burke	0161 244 1216	Catherine.burke@tfgm.com
IS Management Team Representative: IS Lead Service Manager Information Manager Head of Operations Business Applications Manager IS Lead ServiceDesk Manager IS Lead Networks Engineer IS Lead Infrastructure Engineer	 Mat Clayton Aidan Richmond Ricard Fuertes Ian Hull Colin Bernie Jason Higgins Russell Baucutt	 0161 244 1208 0161 244 1123 0161 244 1234 0161 244 1454 0161 244 1234 0161 244 1234 0161 244 1234	 Mat.Clayton@tfgm.com Aidan.Richmond@tfgm.com Ricard.Fuertes@tfgm.com Ian.Hull@tfgm.com Colin.bernie@tfgm.com Jason.higgins@tfgm.com Russell.baucutt@tfgm.com
Head of Information Services	Malcolm Lowe	0161 244 1545	malcolm.lowe@tfgm.com
Internal Audit	David Knight	0161 244 1138	David.Knight@tfgm.com
Communications Team	Daniel	0161 244 0808	Daniel.McMullan@tfgm.com

	McMullan		
Head of Finance	Steve Warrener	0161 244 1025	Steve.Warrener@tfgm.com

External contacts:			
Police	Greater Manchester Police	0161 872 5050	Northampton Rd, Manchester, Greater Manchester M40 5NB
Credit card issuers	Barclays		Pci.taskforce@barclaycard.co.uk
Banks	Barclays Stuart McGarry		Pci.taskforce@barclaycard.co.uk
Information Commissioners' Office		0303 123 1113	Security Breach Notification Form to be emailed to casework@ico.org.uk
Qualified Security Auditors	Sec-1 Wayne Murphy	01924 284240	Waynem@sec-1.com
Financial Services Authority	FSA	020 7066 1000	25 The North Colonnade, Canary Wharf, London E14 5HS

Out of Hours:			
IS Management Team Representative	Malcolm Lowe Ricard Fuertes	07584 616689 07741 833592	Malcolm.lowe@tfgm.com Ricard.Fuertes@tfgm.com

11 Reporting & Communications Strategy

The stages for reporting a perceived, potential or actual breach, intrusion attempt or security incident are:

11.1 Notify a Line Manager within the service area or department. This will assist to observe and record any actions undertaken.

11.2 Report the incident to Information Services. During office hours the initial reporting contact is Serviceline. Out of hours the initial point of contact is the IS Management Team Representative.

11.3 Serviceline will accept the incident, record relevant detail and notify the Lead Security & Compliance Analyst. If the incident is received out of hours, the details will be recorded at the earliest opportunity.

11.4 The Lead Security & Compliance Analyst will work in-conjunction with the reporting officer to conduct an initial assessment, confirm if a breach has occurred and notify the first available IS Manager and the Internal Audit Representative. The IS Manager will then become the nominated IS Management Team Representative.

11.5 The Lead Security & Compliance Analyst will classify the security incident, as defined in section 7, advise an appropriate course of action and commence incident documentation.

11.6 The Lead Security & Compliance Analyst will continue with relevant investigative work and will maintain updates to the IS Management Team Representative.

11.7 The IS Management Team Representative will coordinate efforts by 'owning' the incident. This will involve assigning IS resource to assist the Lead Security & Compliance Analyst; monitoring the production of supporting documentation during and after the incident including the 'lessons learned log'; to authorise any network disconnections; to authorise any electronic and physical 'quarantine' arrangements; to liaise with, and advise, all other IS Managers; to advise internal services of the incident this will include Customer Services, Communications Section, Internal Audit and Legal Services.

11.8 The IS Lead Service Manager will provide frequent update reports to the Head of IS.

11.9 The Head of IS will report all incidents to the Chief Operating Officer, the Director of Finance and other Chief Officers within the organisation, as necessary.

11.10 The Head of IS will, after due consultation with the IS Management Team Representative, the Data Protection Officer and relevant members of the Incident Response Team, decide whether notification to external organisations is appropriate. If so, the notification may be made to any or all of the following external agencies, including, but not limited to, the Police; the Information Commissioners' Office; the external PCI Qualified Security Assessor; banks; credit card agencies.

11.11 The Head of IS will authorise the circulation of any internal advisory notes and any external press releases.

12 Escalation and Notification

12.1 Whilst the defined reporting structure is the primary mechanism to progress an incident there may be occasions when more immediate action is required. At any stage of the incident any officer has the option to escalate activities by referring these directly to the Head of Information Services, who will consider the approach and decide whether a higher priority is appropriate. If so, the Head of IS will advise the IS Management Team Representative.

13 Classification of Security Incidents

The reaction to a reported breach, intrusion attempt or security incident corresponds directly to the potential for damage to the system; data; infrastructure; continued operation of the organisation; reputation of the organisation; or the inappropriate disclosure or modification of data. The Lead Security & Compliance Analyst will determine the classification of a security incident.

The risk levels are characterised as:

13.1 Level 1 Very High Risk Immediate Response

Damage to the system or data is occurring;

Attempts to exploit the vulnerability on that system are occurring;

The vulnerability is currently being actively exploited against other similar technologies within the organisation; probable damage to systems and data is being experienced in those other incidents.

13.2 Level 2 High Risk 1 hour Response

The vulnerability is known to exist on the system;

The exposure is currently being actively exploited against other similar technologies external to the organisation;

Damage to systems and data are being experienced in those other incidents.

13.3 Level 3 Medium Risk 4 hour Response

The system is susceptible to the vulnerability given that the system is configured incorrectly;

The exposure is currently being actively exploited against other similar technologies external to the organisation;

There is some potential for damage to systems and data.

13.4 Level 4 Low Risk 8 hour Response

The system is susceptible to the vulnerability given that the system is configured incorrectly;

The exposure is currently being actively exploited against other similar technologies external to the organisation;

Damage to systems and data is possible but is not considered likely.

13.5 Level 5 False Positive

A False Positive indicates a given condition has occurred, when it actually has not been fulfilled.

This is also referenced as a "false alarm". Where vulnerability is suspected, but investigation confirms it is not considered to be a threat or an incident breach.

14 Incident Response Procedures

The security incident response plan is as follows:

14.1 When a perceived, potential or actual breach, intrusion attempt or security incident is identified, during 'office hours', it must, immediately, be reported to Information Services Serviceline on extension 701234, with further notification to the relevant departmental line manager at the earliest opportunity. Reporting to Serviceline should not be delayed because a manager may not be available. In the event that Serviceline cannot be contacted, the event should be reported to the IS Management Team Representative, or in their absence, to the Lead Security & Compliance Analyst, who will advise the IS Management Team Representative.

14.2 When a perceived, potential or actual breach, intrusion attempt or security incident is identified, outside 'office hours', it must be reported to the on-call representative of the Information Services Management Team**,** with details provided to a line manager, in the service area, at the earliest opportunity via the most convenient method. The Out of Hours contact details for the IS Management Team representative are contained in Section 10.

14.3 The identification of a perceived, potential, or actual breach, intrusion attempt or security incident could result from observation or activity by a person; automated notification from Intrusion Detection System / Intrusion Protection System, File Integrity Monitoring or through Wireless Activity Scanning.

14.4 The IS member of staff receiving notification of the event will report the incident to the IS Co-Coordinating Officer, under normal circumstances this will be the IS Management Team Representative, or in their absence the Lead Security & Compliance Analyst. The reporting structure will then provide notification to the Lead Security & Compliance Analyst or IS Management Team Representative, the IS Management Team, the Head of IS and the Incident Response Team. At the earliest opportunity, they will ensure a Service Incident is recorded.

14.5 The efforts of the Incident Response Team will be coordinated by the IS Management Team Representative, with sufficient resource being allocated to support the Lead Security & Compliance Analyst. The Response Team will investigate the incident and assist the compromised department in limiting the exposure of cardholder data. The Head of IS, in conjunction with the Incident Response Team, shall consider whether, subject to appropriate legal advice and Director authorisation, the activities of the Incident Response Team may include reporting the incident and findings to the appropriate external organisations and agencies.

14.6 The Incident Response Team will work in conjunction with all parties and will cooperate fully with any agencies to ensure the root cause of the security incident is addressed. The Incident Response Team will ensure that all relevant parties are advised of the corrective actions, providing activities are not confidential and will not compromise the reputation of the organisation.

14.7 The Incident Response Team will review the specifics of the incident to determine if policies and processes need to be updated to avoid a similar incident in the future and to complete a lessons learned process to provide future improvements.

14.8 The Incident Response Team will ensure that appropriate formal reporting of the incident and outcomes is undertaken to the Executive Group and Audit Committee.

14.9 Activities to be undertaken by an individual identifying an incident

a) The identifying officer is responsible for the following steps:

b) Report the incident to Serviceline at **TfGM**.

c) Report the incident to a Departmental Manager.

d) Work in-conjunction with the Lead Security & Compliance Analyst to assess, contain and resolve the threat.

e) In conjunction with the Lead Security & Compliance Analyst, to determine the extent of compromise resulting from the event, whether a security breach has occurred and whether there is a suspected or confirmed loss or theft of any material or records that contain credit cardholder data.

14.10 Activities to be undertaken by the Lead Security & Compliance Analyst

a) On receipt of the report of a potential, perceived or actual security breach, to undertake, with the reporting officer, suitably robust initial investigations to determine (a) whether a security breach has occurred and if so, (b) to determine the extent of the impact to the operation of services.

b) If the joint investigation identifies that a security breach has occurred and that credit cardholder data is at risk or has been compromised, the Lead Security & Compliance Analyst will raise a formal Security Incident Response Report, as contained within this document as Appendix 1. This document will be circulated to the IS Management Team Representative; the Incident Response Team; the Head of IS and Head of Audit.

c) The Lead Security & Compliance Analyst will consider all aspects of the situation, to propose immediate actions to protect the organisation; to 'secure' card holder data which may be at risk; to contain the breach and to ensure any associated evidence is not compromised.

d) The Lead Security & Compliance Analyst will remain as the primary investigating officer and will be responsible for establishing the cause of a security breach and identifying the potential resolution.

14.11 Activities to be undertaken by the Incident Response Team

In the event of a perceived, potential or actual security breach, the Head of IS will, if the situation is deemed to be sufficiently serious, form an Incident Response Team and implement the Security Incident response Plan. The 'membership' of the Incident Response Team will vary depending upon the severity of the potential, perceived or actual breach, but has the potential for inclusion of any or all internal **TfGM** services and any or all relevant external organisations.

In response to a compromise, the Incident Response Team will:

a) Ensure the compromised system is quarantined on / from the network.

b) Collate, review and analyse all relevant centrally maintained system, firewall, system integrity, intrusion detection/ protection and activity system logs.

c) Assist the department to collate and analyse locally maintained system and monitoring logs.

d) Conduct technical assessments of the compromised systems, service or infrastructure to establish the extent of the breach. This may involve coordinating the efforts of support organisations to conduct forensic tests to determine any data loss and its' significance in terms of risk or exposure.

e) Report the incident to the Chief Operating Officer and the Director of Finance, who will, inform any relevant external agencies, if it is appropriate to do so.

f) Ensure all collated information is available for examination by approved relevant parties.

g) As required, to assist the investigations by any relevant, approved agency.

h) Ensure all necessary reporting and escalation is undertaken in a timely manner.

i) Ensure the security incident is resolved to the satisfaction of all concerned parties. This will include adhering to any specific requirements defined by the credit card companies, issuers and banks.

j) Ensure a 'lessons learned' activity is undertaken immediately following closure of the security incident.

k) Ensure full supporting documentation is completed and that this is available for inspection by any relevant and approved agency.

l) Activities to be undertaken by Others

m) The Head of Information Services will liaise with other areas of the business.

n) Any 'political' elements resulting from a security incident will be handled by the Director of Finance.

o) The Information Manager will provide expert advice in respect of relevant policies, acts and legislation.

p) Non-technical issues that require notification to external agencies, will be passed, via the Head of IS, to the Communications Team, who can provide official organizational statements, subject to Director authorization.

14.12 Controls available to Information Services

a) In order to protect **TfGM** data and systems, as well as to protect threatened systems external to the organisation, Information Services reserve the authority to remove, quarantine, or place restrictions on technology services provided using any **TfGM** owned systems and networks. Removal of services will be instigated when quarantine, isolation or blocking measures either do not, or are not considered to, apply sufficient protection. Specifically:

b) Limitations may be implemented through the use of policies, standards, and/or technical methods, and could include, but may not be limited to, usage eligibility rules, password requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.

c) Restrictions may be permanently deployed based on a continuing threat or risk after appropriate consultation with affected constituents, or they may be temporarily deployed, without prior coordination, in response to an immediate and serious threat.

d) Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the effect on TfGM functions caused by the restriction approaches or exceeds risk associated with the threat.

e) In order to protect **TfGM** data and systems, as well as to protect threatened systems external to the organisation, Information Services may unilaterally choose to isolate a specific system from an external network, given:

f) Information in-hand reasonably indicates that the system has been compromised.

g) There is ongoing activity associated with the system that is causing or will cause damage to other **TfGM** systems and/or data, or the assets of other internal or external agencies, or where there is a medium-to-high risk of such damage occurring.

h) All reasonable attempts have been made to contact the responsible systems personnel or department management, or such contact has been made where the technician or department managers are unable to, or choose not to, resolve the problem in a reasonable time.

i) Any quarantine measures will be removed when the identified risks are mitigated to an acceptable level, or where loss of access or function caused by the quarantine approaches or exceeds risk associated with the threat.

j) Where changes are required, in an emergency situation, arising from a Security Incident, Information Services will coordinate the retrospective application of ‘Request for Change’.

14.13 Security Incident Reporting

a) During a security incident the normal reporting process will involve the Lead Security & Compliance Analyst and the Incident Response Team advising the IS Management Team Representative of all actions and progress made. It is suggested that the frequency of updates will not exceed 1 hour, even if no progress has been made. A degree of discretion is permissible, if reporting is likely to delay resolution, or if greater urgency requires more immediate notification.

b) The IS Management Team Representative will report to the Head of Information Services. The Head of IS will in turn provide frequent reports to the Chief Operating Officer and the business, including the Director of Finance and Director of Communications Service. It is proposed that the Head of IS will provide supporting technical comment and will notify the contracted Qualified Security Assessors, if assistance or advice is required. The responsibility for advising all other external agencies lies outside Information Systems. This will include notification to the Police, the Press, the banks, credit card agencies and the Financial Services Authority, with such decisions authorised by the Head of IS and the Director of Finance and Corporate Services. The outcome of an incident will be reported to the Executive Group and the Audit Committee.

15 Incident Response Plan – Lessons Learned

a) The major considerations during an incident are to protect card holder data; the card holder data environment and the infrastructure services, including servers and network. Suitable measures will be implemented to protect services, to fully resolve any security issues and then to reinstate operational services. When services are operational and the incident has been fully documented and reported it will be considered to be closed.

b) Immediately, following a security incident a review will be conducted. The process will be coordinated by the IS Management Team Representative, within two working days of closure of the incident. The process will involve a meeting of all parties who had any involvement in the incident, from identification, through investigation to resolution and ultimately closure. The purpose will be to review the cause and effect, to identify action undertaken, positive aspects of the incident, negative aspects of the incident, what was done well and what wasn't. The output from this group meeting will be a full analysis of the incident, which will then be subject to review and will conclude the 'Lessons Learned' exercise and will provide proposed improvements to the Security Incident Response Plan.

The 'Security Incident Lessons Learned Report' is included within this document as Appendix 2.

16 Incident Response Plan - Test Procedure

a) **TfGM**, as an organisational entity and including all **TfGM** employees; **TfGM** Directorates; **TfGM** Operational Units; Service Providers; contractors; partners and any other third parties who may have access to the Card Holder Environment, will undertake robust testing of the Security Incident Response Plan.

b) On an annual basis, IS staff, acting as representatives of an Incident Response Team, will prepare a simulated security incident and will test this incident against the Security Incident Response Plan.

c) The simulated security incident will be considered to compromise customer credit card data. The simulated incident must be of severity level 1 or 2 and considered to present a high risk to the organisation. This simulation must consider a minimum of one of the following essential scenarios, Intrusion Detection System / Intrusion Protection System alerts; File Integrity Monitoring alerts; Rogue Wireless Access Points; Evidence of unauthorised activity (Version 3); Alert from Payment Brand.

The process for testing the Security Response Plan will include:

16.1 Notifying appropriate management staff in advance and scheduling a date to begin the test.

16.2 Establish and communicate the protocols that will distinguish the test from a real security incident.

16.3 **TfGM** staff will be required to detect the incident and to respond in accordance with the activities defined in this document.

16.4 The Head of Information Services will ensure the completion of an incident response report to evaluate the test's success.

16.5 The report will include observations and comments from those who participated.

The test will be considered as successful if:

- All involved completed their assigned role without delays or problems.

- The response communication was effective and without delays.
- The response procedure was found to be complete and functional, with no or very minimal flaws.
- The simulated adverse effect to staff, operations, data, and property caused by the incident was limited to the minimum possible by the response procedure.
- Additional security vulnerabilities revealed by the test are minor, with minimal potential impact.

16.6 The test will be considered to have failed if:

- Two or more employees were unable to complete their assigned tasks without delays, or if problems were encountered.
- Response communication failed at any stage.
- The test revealed significant deficiencies or problems in the response procedure.
- The response procedure indicated that adverse effects to staff, operations, data, and property, which are considered to be unreasonable, may have occurred.
- The test revealed security vulnerabilities that could have adverse effects on staff, data, or property.

16.7 The Head of Information Services will ensure that necessary amendments to the response plan or staff training are identified and addressed. If the incident response failed, a re-test will be carried out after procedures have been improved and staff training completed.

The Head of Information Services will ensure that:

- Necessary changes to the Incident Response Plan and supporting procedures are implemented within 30 days of the response plan test.
- Necessary training for staff is undertaken within 45 days of the response plan test.

If the initial test failed, a re-test must be carried out within 60 days of the initial test and after required changes to procedure have been made and staff have received additional training.

17 Incident Response Plan – Test Scenarios

In addition to inclusion within the Incident Response Plan Test Procedure Simulated Incident, compliance requires that the following are to be tested at regular intervals, with all essential elements tested on an annual basis.

- Cyber Security Incidents
- File Integrity Monitoring alerts
- Denial of Service
- Evidence of unauthorised activity (Version 3)
- Alert from Payment Brand

17.1 Cyber Security Incident

a) Testing is completed within an annual training program within IS Serviceline to ensure Cyber Security Incidents are logged correctly, procedure is up-to-date and staff are trained.
b) Cyber Security Incident annual review, unless any changes take place. Updated and communicated to IS Serviceline.

17.2 File Integrity Monitoring

a) Testing is completed on an annual basis.
b) Logged events are then identified on the next morning's daily report. This provides a degree of confidence that file integrity monitoring detections are dynamic as it reflects a controlled change to the environment. Therefore, other identified changes are considered for further investigation.

17.3 Denial of Service Attack

a) Testing is completed on an annual basis.
b) A flood of traffic taking down a website, can apply to phone lines, or other web facing systems, in some cases internal systems.

17.4 Evidence of unauthorised activity

a) This scenario will consider a primary issue of unauthorised credit card activity, with suspicious transactions reported by a member of the public, following notification of suspicious use from their bank.

b) The scenario will assume misuse of credit card detail. The initial contact from the card owner will be through the Customer Services Contact Centre or Drivesafe.
c) The scenario will involve participation by the receiving section, IS, Internal Audit and simulated communication with relevant external agencies, such as the Police and the card issuing bank.
d) The scenario will be designed to test containment, information security, incident response reaction and evidence gathering. A full lesson learned exercise will be undertaken, with impacts full detailed and applied to future releases of this plan.

17.5 Alert from Payment Brand

a) This scenario will be designed around an official alert received from bank.
b) The scenario will consider that multiple instances of credit card misuse have been identified, by the bank and that a common source of information loss has been traced to **TfGM**.
c) The exercise will consider the notification process from the bank; the incident response reaction; the internal notification procedures; the actions of the participating groups to contain the situation; the organisation's use of forensic investigators and the organisation's communication with external agencies such as the Information Commissioners' Office, The Police and the bank.
d) The purpose of this scenario is to rehearse the activities that will be required in the event that notification of misuse is received.
e) A full lesson learned exercise will be undertaken, with impacts fully detailed and applied to future releases of this plan.

18 Incident Response Plan – Revision

a) The **TfGM** Incident Response Plan will be reviewed and possibly revised:
   - Within 12 months of the most recent revision
   - After a real major security incident
   - After any failed test of the security incident response plan
   - Following a monitoring review by Internal Audit

The Incident Response Plan review must consider;

- Industry development;
- all internal and external influences including industry best practice, including knowledge from Government and EU Cert teams; Internet Engineering Task Force (IEFT);
- NIST and legal requirements that may be adopted, such as the proposed breach notification laws.

Revisions to the Incident Response Plan must be reviewed and approved by the Head of Information Services.

19 PCI DSS Incidents

PCI related incidents will be reported to ServiceLine, where they will be logged under the call type 'Security Issue', within the category 'PCI DSS', with detail of 'PCI DSS Security Issue'.

a) Serviceline will report the incident, in the first instance, to the IS Incident Co-ordinator, under normal circumstances the co-ordinator will be the IS Management Team Representative.
b) If the primary IS Management Team representative is unavailable, the incident should be reported to an alternative Management Team representative.
c) If no Management Representatives are immediately available then the incident should be reported to the Lead Security & Compliance Analyst, with retrospective notification to the IS Management team Representative.
d) The absence of a Management Team representative should not delay the process of investigation.

At quarterly intervals a detailed report of all PCI DSS calls will be produced from the Heat system by the IS Service Manager. This report will be reviewed by the IS Co-ordinator to identify any threat patterns and a summary will be reported to the Head of IS.

20 Business Continuity

a) A project to develop an Information Services Business Continuity Manual and Disaster Recovery Manual is currently proposed. The following is provided as advice for the intervening period.

Business Continuity - Responding to a Level 1 Security Incident

b) In response to a Level 1 Security Incident, specifically relating to credit card holder data, TfGM or one of its' operating partners or Service Providers may temporarily close premises in order to conduct corrective actions, reinstatement of services or investigations of a perceived, potential or actual breach. Depending on the nature of the incident, the closure could last from a few days to a few months.
c) The Head of Information Services will provide instructions and guidance to Information Services staff on how, when, and where to restore mission critical operations. Critical operations may be continued, degraded, or suspended.

To prepare for a Level 1 incident, all employees should:

d) Keep copies of contact lists; Security Incident Response Plan and supporting procedures; relevant Business Continuity and Disaster Recovery manuals at home.
e) Be prepared to work from home where this is possible;
f) Be prepared to relocate to a different temporary work base, that is not affected.
g) While the office is closed all employees should check in daily with line managers until instructed otherwise.

Business Continuity - Responding to a Level 2 Security Incident

h) In response to a Level-2 incident, the **TfGM** offices remain open but PCI-data or systems are affected. This could cause a temporary shut-down of credit card processing.
i) The Head of Information Services will provide instructions to staff.

Business Continuity - Responding to a Level 3 Security Incident

j) In a Level 3 incident, the **TfGM** offices remain open but business operations are adversely affected somehow. In a Level 3 incident these adverse effects do not compromise PCI data, however the potential is evident and has been identified outside the organization.

k) Level 3 incidents can be varied and difficult to predict, so business continuity will depend on the nature of the incident and the resources that are available.
l) The Head of Information Services will provide direction and guidance to staff on how to proceed.
m) Tasks and solutions could include, but are not limited to, taking preventative or avoiding actions; protecting the environment; researching reporting incidents; undertaking specific risk assessments.
n) Ensuring completion of system backups, with secure copies stored offsite.
o) All staff should maintain operating records detailing actions to be undertaken to ensure the continuation of critical business services. These documents should consider how services will be supported in the event that normal computing facilities and network resources become unavailable.

21 Legal Implications

a) A failure to implement proper controls on card payment data and/or a security breach could put **TfGM** in breach of data protection laws.
b) In the event of such a breach there are a number of enforcement actions that may be taken against **TfGM** by the Information Commissioners Office (ICO). For serious breaches the ICO can impose a fine of up £500,000 and prosecute anyone who commits a criminal offence.
c) By accepting card payments **TfGM** is required to subscribe to the Data Security Standards of the Payment Card Industry.
d) These standards require **TfGM** to implement control procedures and processes. If, in the event of a security breach, it is found that **TfGM** were not compliant with these standards then **TfGM** may be subject to penalties which can include a fine or termination of card payment services.

22 Audit Review

From time to time, Internal Audit will review the operation of this plan and other associated security controls. A report will be issued to IS Management

advising of the results of work undertaken, highlighting any control weaknesses and providing recommendations for control improvement, as appropriate.

23 Appendix 1 -Security Incident Response Report

SECURITY INCIDENT RESPONSE REPORT

INCIDENT IDENTIFICATION INFORMATION	
Date and time of notification:	
Status:	
Incident Reference:	
LEAD BY	**REPORTED BY**
Name:	**Name:**
Title:	**Title:**
Contact Information:	**Contact Information:**

INCIDENT SUMMARY			
Severity:		**Location:**	
Type of incident Detected:			
☐Denial of Service	☐Unauthorised Access	☐Unplanned Downtime	
☐Malicious Attack	☐Unauthorised Use	☐Other	
Description of Incident:			
Affected Systems:		**User Groups Affected:**	
Experienced Downtime:			
Service	**Dates/Times**	**Details**	**Affected Users**

INCIDENT NOTIFICATION		
☐IS Management	☐ Director of IS	☐Application/System Supplier
☐IS Team	☐ Director of Finance	☐Affected Users
☐Lead Security & Compliance Analyst	☐ Application/System Owner	☐Audit
☐Communications / External organisations:		
Names and Contacts of Persons Involved		

WORKFLOW SUMMARY		
Date	**Time**	**Details**

ACTION SUMMARY
Identification Measures:
Containment Measures:
Evidence Collected:
Corrective Measures:
Back-out Strategy:
Other Mitigating Actions:

24 Appendix 2 - Lessons Learned Report

SECURITY INCIDENT LESSONS LEARNED REPORT

INCIDENT IDENTIFICATION INFORMATION			
Date and time of notification:			
Status:			
Incident Reference:			
LEAD BY	**REVIEW TEAM**		
Name:			
Title:			
Contact Information:			

POST INCIDENT ANALYSIS
Incident Summary:
Cause of Incident:

Damage Caused:

Actions:

Action	Status	Assigned:	Team:	System Reference	Date Raised	Date Completed

Lessons Learned:

Improvements to the Incident Response Plan:

25 Appendix 3 - Advisory Notes

Advisory notes to support and assist in the discharge of activities during an incident.

a) Remain calm. Consider all activities and any course of action. Involve a second person to assist, observe and advise.

b) Conduct a methodical assessment of the situation. Do not simply shut services down or immediately power equipment off, as valuable monitoring information may be lost. If the server or PCs are being used to attack others, or if the attacker is actively using or damaging the machine, it may be necessary to disconnect it from the network.

c) Report the problem. Contact IS Serviceline or the Lead Security & Compliance Analyst and request emergency assistance to investigate a security incident.

d) Collate all relevant information. This may include, but is not limited to, system logs, directory listings, electronic mail files, screen prints of error messages, and database activity logs. Copy them to a safe location, where they will not be deleted or over-written.

e) Document all events, actions and activities. Ensure all relevant information is recorded, including observations; actions taken; dates and times; staff involved. If in doubt, ensure information is recorded, preferably as it occurs. Over time, activities and actions and the order in which they occurred will not easily be remembered. The preservation of information is critical to any legal action that may take place at a later date.

f) Change account passwords. All system accounts that were involved with the incident should have new passwords. Exceptions to this rule are accounts which are authenticated with tokens or certificates, in which case the PIN or pass-phrase should be changed.

g) Change the status of accounts, if necessary. In the event that a system administrator detects a problem with a system, or user activity on a system, a quick way to stop the unwanted activity is to "close" an account, by restricting logins to it. This results in the account owner having to contact an administrator in order to remove the login restriction. This is not deleting the account, but is merely making the account temporarily unusable.

h) Stop rogue service(s). In the event that a system compromise or denial-of-service attack is underway, where it cannot be stopped or the service 'killed', it may be necessary to disconnect equipment from the network.

i) Ensure effective backup policies are enforced. If data and/or the operating system have been compromised, it will be necessary to ensure that a "clean" backup is available for restoration. If not managed correctly, it is possible that the next backup could overwrite an undamaged backup, immediate steps should be taken to prevent that occurrence. Policies should include multiple levels of backup, and you are uncertain how long the system has been compromised, you must determine which backup to version restore to. Until that time, do not allow any backups to be overwritten.

j) Actions to effect a repair or reinstate a service. The appropriateness of each course of action varies with the severity of the incident, (amount of damage, legal implications, cost of recovery, etc) and in the case of department-owned systems, the department policy. Information Services will offer advice to support a decision. The department managing a service or system that has had an incident, has been compromised or breached is ultimately responsible for ensuring that any legal actions are not compromised by restoring or reinstatement of services. Advice should be sought from Legal Services.

Transport for Greater Manchester

Appendix 4 - Incident Review Threat Patterns

SECURITY INCIDENT THREAT PATTERN REVIEW

INCIDENT REVIEW INFORMATION			
Date and time of Review:			
Quarterly Period:			
REVIEW LEAD	**REVIEW TEAM**		
Name:			
Title:			
Contact:			

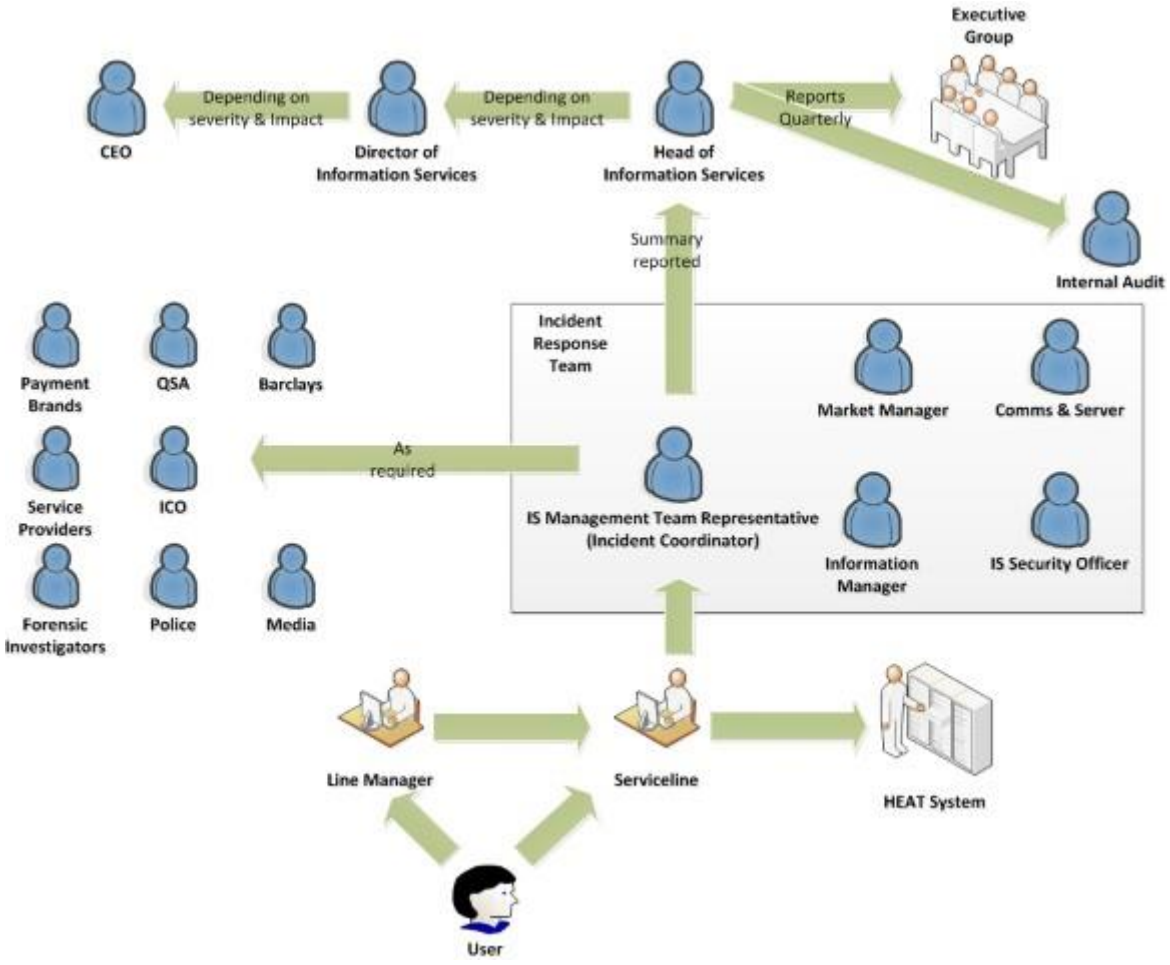
POST INCIDENT ANALYSIS
Summary of Incidents:
Incident Patterns:
Reoccurring Root Cause:

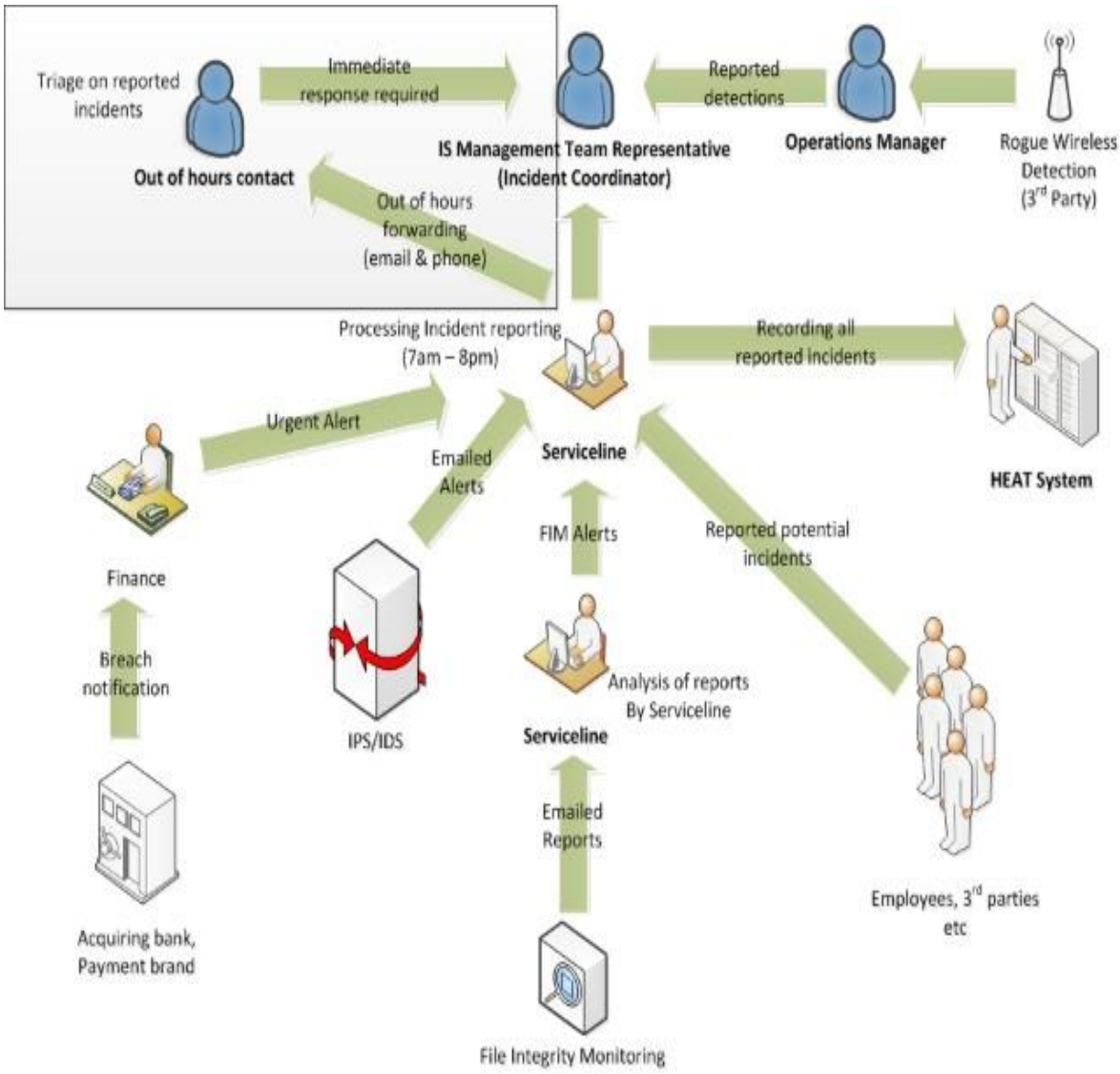
Actions to reduce Cause:

Action	Status	Assigned:	Team:	System Reference	Date Raised	Date Completed

Update:

26 Appendix 5 - Security Incident Response Plan Process Diagrams


Executive Group
CEO
Depending on severity & Impact
Director of Information Services
Depending on severity & Impact
Head of Information Services
Reports Quarterly
Internal Audit
Summary reported
Incident Response Team
Market Manager
Comms & Server
Payment Brands
QSA
Barclays
As required
Service Providers
ICO
IS Management Team Representative (Incident Coordinator)
Information Manager
IS Security Officer
Forensic Investigators
Police
Media
Line Manager
Serviceline
HEAT System
User


Triage on reported incidents
Immediate response required
Out of hours contact
IS Management Team Representative (Incident Coordinator)
Reported detections
Operations Manager
Rogue Wireless Detection (3rd Party)
Out of hours forwarding (email & phone)
Processing Incident reporting (7am – 8pm)
Recording all reported incidents
HEAT System
Urgent Alert
Emailed Alerts
Serviceline
FIM Alerts
Reported potential incidents
Finance
Breach notification
IPS/IDS
Analysis of reports By Serviceline
Serviceline
Acquiring bank, Payment brand
Emailed Reports
Employees, 3rd parties etc
File Integrity Monitoring

27 Appendix 6 – Common Scenarios

The following scenarios have been identified as possibilities within the annual Risk Assessments. These are included to reference the actions that need to be undertaken should any of the following arise.

Threat: Fire Alarm

Scenario:
After a fire evacuation, upon returning to office, the office door appears to have been forced and some forms containing data are missing

Actions:

- Avoid touching anything, so as not to compromise any evidence.
- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Major Accident

Scenario:
Following a major accident I ran out of the Travelshop to administer first aid. Upon return to the office I realised the door was not properly secured and it looks like someone was in the office and has removed some paperwork which had credit card details on it.

Actions:

- Avoid touching anything, so as not to compromise any evidence.
- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Loss of Power

Scenario:
We had a power cut in the office, and as I was unable to input the data from today's forms, I went to lunch early and completely forgot to lock away the forms, upon my return, they appear to be missing.

Actions:

- Avoid touching anything, so as not to compromise any evidence.
- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Remote Spying

Scenario:
I've found a suspicious device in the data centre which looks like a camera, which might be recording what I'm doing on my PC.

Actions:

- Avoid touching anything, so as not to compromise any evidence.
- Notify your manager.
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Eves Dropping

Scenario:
Whilst I was taking a call, when I was reading back the card number, I suspect one of my colleagues was recording my voice. He had a device that looked like a voice recorder

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Theft of Media or Documents

Scenario:
After receiving the post this morning, before I was able to process it, I got called away urgently, and upon my return some or all of it was missing. I suspect an opportunist thief has stolen it.

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Retrieval of Recycled or Discarded Material

Scenario:
I was shredding some forms and I got distracted by a colleague who needed urgent assistance with a customer query. In my absence someone has removed the forms.

Actions:

- Avoid touching anything, so as not to compromise any evidence.
- Notify your manager.
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Disclosure

Scenario:
I left my desk to get a print off the printer, upon my return it looked like a stranger was taking photos of some forms with credit card data on them.

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.
- Jot down a description of the person whilst fresh in your mind

Threat: Data from Untrustworthy Source

Scenario:
I've had a virus alert during the weekly scheduled scan. It says it's a key-logger. I've not been on the internet at all today, I can't imagine how it got there.

Actions:

- Discontinue use, so as not to compromise any evidence, do not switch off.
- Notify your manager.
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Tampering with Hardware (1)

Scenario:
There's a strange device attached to my PC base unit, I'm sure it wasn't there before.

Actions:

- Avoid touching anything, so as not to compromise any evidence.
- Notify your manager.
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Tampering with Hardware (2)

Scenario:
I've just noticed something attached to the Paypoint/PDQ machine, I'm sure it shouldn't be there.

Actions:

- Discontinue use, so as not to compromise any evidence, do not switch off.
- Notify your manager.
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Tampering with Software

Scenario:
I've just logged on to a colleagues PC as mine isn't working and there is a strange program installed that wouldn't normally be on one of our PC's. I think my colleague is doing something that he shouldn't.

Actions:

- Discontinue use, so as not to compromise any evidence, do not switch off.
- Notify your manager.
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Error in Use

Scenario:
I was in a rush to get to Marks, before I got my usual train and I've left some unprocessed forms on my desk.

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Hacker Cracker

Scenario:
An Engineer has just turned up that we are not expecting, he seems to have a good knowledge of the layout of the building and knows a few names and is insistent the person said to let reception to know it was OK for him to go straight up, as he's been before and knows where he is going.

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Insiders (1)

Scenario:
My colleague is behaving a bit shiftily whilst processing forms. It looked like he was writing down the numbers, when he has no need to.

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Insiders (2)

Scenario:
My colleague is always logged in to her hotmail account, I'm sure I saw her typing in numbers when she was processing forms.

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Insufficient Security Training / Security Awareness (1)

Scenario:
I was looking at a shopping website on my break and I kept getting this prompt, which wouldn't go away until I clicked yes. Now my PC is running slowly and I think it may be infected with a virus or something.

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Insufficient Security Training / Security Awareness (2)

Scenario:
My friend sent me an email this morning with a link to a funny video. When I clicked on the link, nothing happened and now my PC is misbehaving.

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Organisational Change – Loss of Staff (1)

Scenario:
I've just found out one of new guy's was sacked from his last job for stealing. One of my friends knows him, should I say anything

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

Threat: Organisational Change – Loss of Staff (2)

Scenario:
I've just had a phone call from Barclaycard to say we have had a data breach. A number of compromised cards have been traced back to one of our call centres. The payments were all taken during the last 6 months at **TfGM**. A pattern has emerged over a 6 month period

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

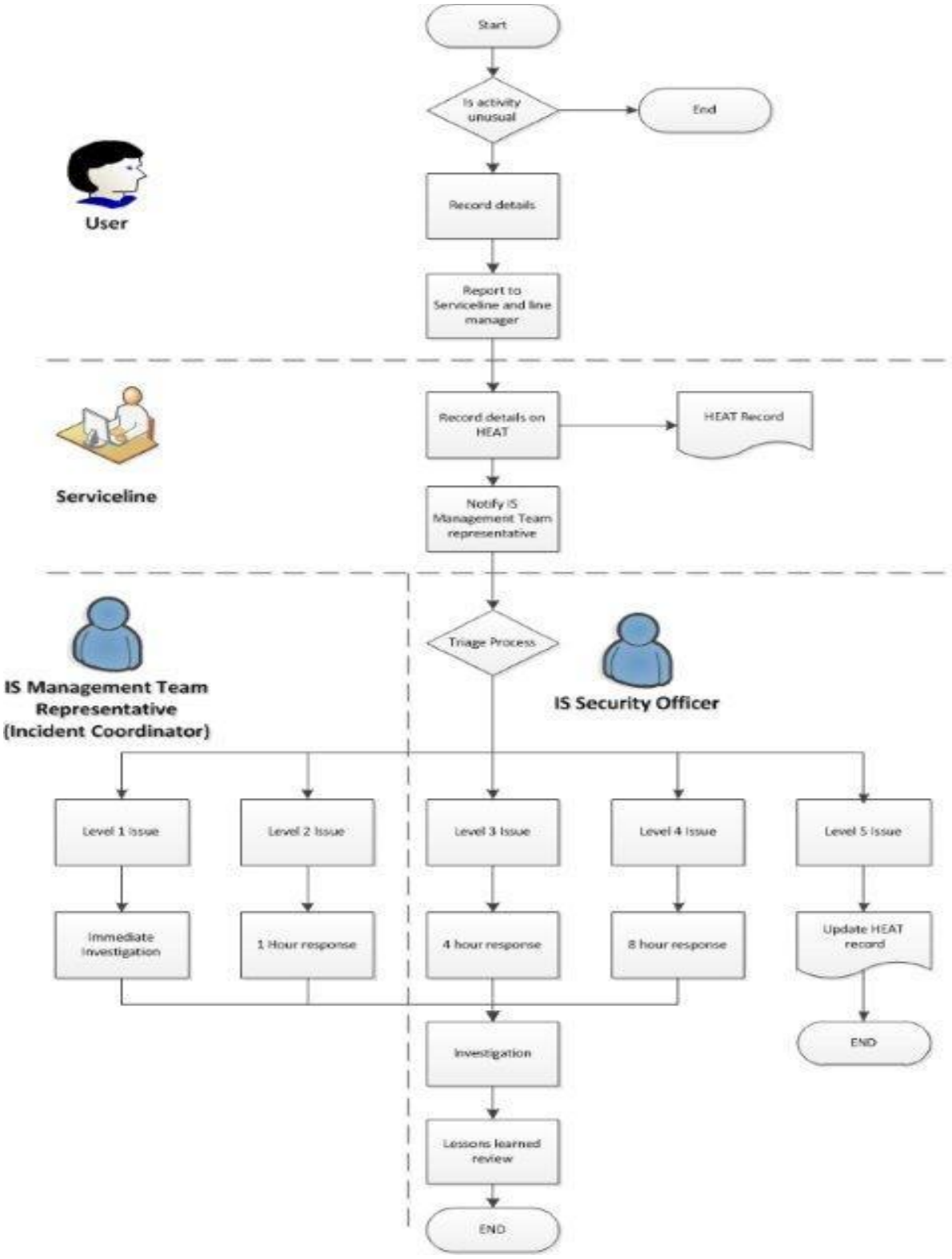
Threat: Organisational Change Loss of Staff (3)

Scenario:
Our website which re-directs users to take payments looks like it has changed slightly

Actions:

- Notify your manager if available
- Ensure that the incident is reported to Serviceline immediately and await further instructions.

28 Appendix 7 - Guidance – Process Diagram



29 Appendix 8 - References

Documents:

The IS Disaster Recovery & Security Incident Response Policy PO3

The Information Services Disaster Recovery Plan

The Information Services Business Continuity Plan

TfGM Business Continuity Plan

TfGM IS Risk Assessment

Procedures:

The Security Incident Management Procedure PR08

Wireless Networks – Investigation of Security Incidents

Wireless Networks – Security Breach Resolution Procedure

Information Security Breach Procedure

Security Incident Response Plan Testing Procedure

Lessons Learned Procedure

Security Incident Threat Pattern Review

Forms:

Security Incident Response Report

Security Incident Lessons Learned Report

Security Incident Threat Pattern Review

30 Glossary and References

Glossary

See document - P99 - Glossary

Policy: Security Incident Response Plan				
Version	**Change**	**Reason for change**	**Date**	**Name**
1.0		Initial Version	30/10/2012	G. Bradley
2.0	Annually Review	No Change	30/10/2013	G. Bradley
3.0	Annually Review	No Change	30/10/2014	G. Bradley
4.0	Annual Review – Change in Template	Review and Template	21/10/2015	C. Burke
5.0	Date and version	Annual Review	31/03/2016	C. Burke
6.0	Name Change	Change in Incident Response Team	01/11/2016	C.Burke
7.0	Annual review/New Head of IS	Annual Review	31/03/2017	C. Burke
8.0	Version and Date	Annual Review	31/03/2018	C. Styler
8.0	Version and Date	Annual Review	31/03/2019	C. Burke
8.1	Operations Manager	Annual Review	31/03/2020	C. Burke
8.1	Version & Date	Annual Review	31/03/2021	C. Burke
8.2	Update Plan	Change of names & Test Plan	12/10/2021	C. Burke