Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Incident & Response Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31st March 2019	Document Reference no.	IS Incident & Response Policy Ref No. 014
Version No.	7.0	Prepared by:	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) 31st March 2019		Implementation date: 31st March 2019 Annual review date: 31st January 2020

Table of Contents

1 Policy Aims

a. This policy is intended to ensure that **TfGM** is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents.

b. Note that this policy is not intended to provide a substitute for legal advice, and approaches the topic from a security practices perspective.

2 Policy Scope

a) A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data.

b) This policy covers all incidents that may affect the security and integrity of **TfGM** information assets, and outlines steps to take in the event of such an incident to ensure successful recovery.

c) The scope of this policy covers all information assets owned or provided by **TfGM**, whether they reside on **TfGM's** network or elsewhere.

3 Policy Delivery

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

4 Accountability

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

5 Policy Monitoring/ Compliance

a) This policy will be enforced by the Executive.

b) Information including logon dates, times, usage duration and device identity will be logged and maybe used for monitoring purposes, and 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.

d) In extreme circumstances Audit & Assurance may access equipment or information to help support investigations.

6 Incident & Response Policy

6.1 Types of Incidents

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

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 Trojan or malware infection.

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.

All security incidents must be reported immediately to the IS Service Desk.

7 Preparation

a) Work done prior to a security incident is arguably more important than work done after an incident is discovered. It is essential to maintain good security controls that will prevent or limit damage in the event of an incident.

b) This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops and mobile devices.

c) Additionally, prior to an incident, TfGM must ensure that the following is clear to IS personnel:

- What actions to take when an incident is suspected.
- Who is responsible for responding to an incident.

d) Reviews of all industry or governmental regulations that dictate how it must respond to a security incident (specifically, loss of customer data) must be performed periodically to ensure the incident response plans adheres to these regulations.

8 Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers.

9 Electronic Incidents

When an electronic incident is suspected and reported to the IS Service Desk, **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:

1. Remove the compromised device from the network by unplugging or disabling the network connection. Do not power down the machine.
2. Disable the compromised account(s) as appropriate.
3. Report the incident to the IS Operations Manager.
4. Backup all data and logs on the machine, or copy/image the machine to another system.
5. 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?
6. Notify the Head of IS and management/executives as appropriate.
7. Contact an IS Security consultant.
8. Determine how the attacker gained access and disable this access.
9. Rebuild the system, including a complete operating system reinstall.
10. Restore any needed data from the last known good backup and put the system back online.
11. Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.

12. 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.
13. Review work instructions procedures and policies and make any amendments as required.

10 Physical Incidents

a) To mitigate the impact of physical security incidents it is mandated to use strong encryption to secure data on all laptops and password protect all mobile devices. Applicable polices, such as those covering encryption and confidential data, should also be read in conjunction with this policy.

b) Physical security incidents are most likely the result of a random theft or inadvertent loss by a user, but they must be treated as if they were targeted at the **TFGM**.

c) **TfGM** must assume that such a loss will occur at some point, and periodically survey a random sampling of laptops and mobile devices to determine the risk if one were to be lost or stolen.

Establish the severity of the incident by determining the data stored on the missing device. Two important questions must be answered:

1. Was confidential data involved?
2. Was strong encryption used?

11 Loss Contained

In the event of a loss being reported the following items that were stored on the lost system must be changed immediately:

- Usernames
- Passwords
- account information
- WEP/WPA keys
- passphrases

The Head of IS and the applicable authorities must be notified that a theft has occurred.

12 Data Loss Suspected

a) In the event of a loss being reported the following people must be notified immediately so that each team can evaluate and prepare a response.

   - an Executive Director
   - Head of Legal Services
   - Head of Media
   - Head of IS

b) The Head of IS and the applicable authorities must be notified that a theft has occurred.

c) Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

13 Notification

If an electronic or physical security incident is suspected to have resulted in the loss of third-party or customer data then the applicable regulations relating to the type of data and or breach disclosure laws must be reviewed and followed as appropriate.

14 Enforcement

This policy will be enforced by the Executive and violations may result in disciplinary action in accordance with TfGM disciplinary policy.

15 Definitions

Encryption: The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Malware: Short for "malicious software." A software application designed with malicious intent. Viruses and Trojans are common examples of malware.

Mobile Device: A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

PDA: Stands for Personal Digital Assistant. A portable device that stores and organises personal information, such as contact information, calendar, and notes.

Smartphone: A mobile telephone that offers additional applications, such as PDA functions and email.

Trojan: Also called a "Trojan Horse." An application that is disguised as something innocuous or legitimate, but harbours a malicious payload. Trojans can be used to covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts.

Virus: Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

WEP :Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WPA: Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

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

Policy/Procedure:				
Version	Change	Reason for change	Date	Name
3.0	Date and Version	Annual Review	31/03/2014	C Burke
4.0	Date and Version	Annual Review	30/04/2015	C Burke
5.0	Date and Version	Annual Review	31/03/2016	C Burke
6.0	Date and Version	Annual Review, New Head of IS	31/03/2017	C Burke
7.0	Date and Version	Annual Review	31/03/2018	C. Styler
8.0	Date and Version	Annual Review	31/03/2019	C. Styler