Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Security Patching 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 Security Patching Policy Ref No. 024
Version No.	6.0	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 outlines the standard of patching required to mitigate the risk of known vulnerabilities being exploited in **TfGM** systems.
b) Vulnerabilities are weaknesses in software that can be exploited by a malicious entity to gain greater access and/or permission than it is authorised to have on a computer.
c) Timely patching is critical to maintain the operational availability, confidentiality, and integrity of computer based information systems.

2 Policy Scope

a) This policy is primarily aimed at **TfGM** systems administrators and technical support staff, who are responsible for the development and maintenance of TfGM IS facilities.

b) Applicability extends to any third party support companies who undertake activities governed by this policy.

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 Operations
- **Awareness:** IS Department

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 Policy

a) All **TfGM** computer systems that connect to **TfGM's** network, regardless of operating system, including routers and switches, are to be protected both from malicious code and hacking attacks which exploit software vulnerabilities, through the deployment and installation of operating system security patches.

b) Critical security patches must be installed universally across applicable **TfGM** computers, when they become available, in accordance with this policy.

6.1 Patch Sourcing

a) Microsoft Patches should be downloaded automatically from the authorised Microsoft Windows update web site, via an approved WSUS server.

b) Staff who are responsible for the maintenance of desktop machines and servers than run operating systems and applications other than those that are Microsoft based, are required to subscribe to the appropriate security mailing services of their respective technology providers, so that they are kept up to date with details of vulnerabilities, exploits and patches associated with their particular platform.

c) An organisational hardware and software inventory should be maintained to identify relevant patch requirements.

6.2 Desktop Patching

All desktop computers that are accessible from the **TfGM** network must be fully patched up to date.

Processes and procedures must be in place to ensure that:-

1. All patches are approved by the Change Advisory Board (CAB) prior to application.

2. Major version upgrades should be fully tested prior to release i.e. service packs or Internet Explorer versions.
3. PC's are automatically updated, using WSUS for Microsoft patches and configuration Manager for other applications, unless running under APP-V.
4. Critical security patches are deployed within 30 days of release.
5. All other patches deployed within 90 days of release

6.3 Server Patching

Servers running Microsoft Operating systems must be fully patched up to date.

Processes and procedures must be in place to ensure that:-

1. All patches are approved by the Change Advisory Board (CAB) prior to application.
2. Patches are fully tested in the development environment prior to being applied to the live environment.
3. All server patches should be applied manually in a controlled manner.
4. Patches to critical systems are applied out of hours to minimise down time.
5. Critical security patches are deployed within 30 days of release.
6. All other patches deployed within 90 days of release.

6.4 Laptops and Occasional Network Attached Computers

It is the responsibility of the staff member to whom the device has been issued to ensure that it is regularly switched on and attached to the network to ensure that all security patches are applied.

Where it is necessary for a device to be away from the network for extended periods, IS should be consulted so that automatic updates can be configured.

6.5 Patching of Routers and Switches

a) **TfGM** Network Management staff will subscribe to appropriate security alert e-mailing lists and proactively monitor appropriate web sites for notification of any vulnerabilities affecting routers and switches.
b) Where vulnerabilities are found to apply to **TfGM** network devices, advice will be sought from **TfGM's** third party network support contractor to determine

whether it is feasible to use a work-around solution rather than apply a patch immediately.

c) Where possible the application of patches will be deferred until the next available scheduled maintenance slot. However, where deferment is not advisable, a risk assessment will be carried out and remedial action will be taken, following local procedures which are designed to minimise disruption.

6.6 Other Vulnerability Mitigation

Not all vulnerabilities have related patches. In such circumstances security officers must find information on and advise system administrators of mitigating “unpatched” vulnerabilities through other methods (e.g. workarounds, firewalls, and router access control lists).

7 Definitions

APP-V: Microsoft Application Virtualisation is an application utilisation and application streaming solution from Microsoft.

Firewalls: Is a device or set of devices, designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect the network from unauthorised access.

Patches: A patch is a piece of software designed to fix problems, with or update a computer program or its supporting data.

Router: is a device that forwards data packets across computer networks. Routers perform the data ‘traffic direction’ functions on the Internet.

WSUS Server: (Windows Server Update Services) provides a software update service for Microsoft Windows operating systems and other Microsoft software.

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

Policy/Procedure:				
Version	**Change**	**Reason for change**	**Date**	**Name**
1.0	Date and Version	Annual Review	06/03/2014	C Burke
2.0	Date and Version	Annual review	30/04/2015	C Burke
3.0	Date and Version	Annual Review	31/03/2016	C Burke
4.0	Date and Version	Annual Review, new Head of IS	31/03/2017	C Burke
5.0	Date and Version	Annual Review	31/03/2018	C Styler
6.0	Date and Version	Annual Review	31/03/2019	C Styler