Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Third Party Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	6th March 2014	Document Reference no.	IS Third Party Policy Ref No. 026
Version No.	3.0	Prepared by:	Catherine Burke/Jude Singleton
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:	IS Director		Implementation date: 31st March 2014 Annual review date: 31st January 2015

Table of Contents

1 Policy Aims

This policy ensures the implementation of a direct third party connections are secure, controlled and monitored.

2 Policy Scope

Direct connections to external entities are sometimes required for business operations. These connections are typically to provide access to vendors or customers for service delivery.

Since **TfGM's** security policies and controls do not extend to the users of third party networks, these connections can present a significant risk to the network and thus require careful consideration.

The scope of this policy covers all direct connections to **TfGM's** network from non-**TfGM** owned networks. The policy excludes remote access and Virtual Private Network (VPN) access, which are covered within separate policies.

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:** IS Director
- **Compliance:** IS Operations
- **Awareness:** IS Department

5 Policy Monitoring/ Compliance

Monitoring and compliance will be provided by the existing firewall or from the Access List report, should a breach of policy be identified, it may be used in disciplinary proceedings.

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

6.1 Use of Third Party Connections

a) Third party connections are to be discouraged and used only if there are no other reasonable options available.

b) When is it necessary to grant access to a third party, the access must be restricted and carefully controlled.

c) A requester of a third party connection must demonstrate a compelling business need for the connection. This request must be approved by the Head of IS or the IS Director.

6.2 Security of Third Party Access

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

1. Connections to third parties must use a firewall or Access Control List (ACL) to separate the **TFGM** network from the third party's network.
2. Third parties will be provided only the minimum access necessary to perform the function requiring access. If possible this should include time-of-day restrictions to limit access to only the hours when such access is required.
3. Wherever possible, systems requiring third party access should be placed in a public network segment or demilitarized zone (DMZ) in order to protect internal network resources.
4. If a third party connection is deemed to be a serious security risk, the Head of IS will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures should be taken at the discretion of the Head of IS or IS Director.
5. Third party access must be discussed with IS Management to agreement

being reached.

6.3 Restricting Third Party Access

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

1. Restrict access to **TfGM's** network to only those users that have a legitimate business need for access.
2. Provide **TfGM** with the names and any other requested information about individuals that will have access to the connection. **TfGM** reserves the right to approve or deny this access based on its risk assessment of the connection.
3. Supply **TfGM** with on-hours and off-hours contact information for the person or persons responsible for the connection.
4. (If confidential data is involved) Provide **TfGM** with the names and any other requested information about individuals that will have access to the confidential data. The steward or owner of the confidential data will have the right to approve or deny this access for any reason.

6.4 Auditing of Connections

In order to ensure that third-party connections are in compliance with this policy, they must be audited annually.

7 Applicability of Other Policies

This document is part of **TfGM's** cohesive set of IS policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

8 Enforcement

9 Definitions

Access Control List (ACL): A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

Demilitarized Zone (DMZ): A perimeter network, typically inside the firewall but external to the private or protected network, where publicly-accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.

Firewall: A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Third Party Connection: A direct connection to a party external to the company. Examples of third party connections include connections to customers, vendors, partners, or suppliers.

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

Policy/Procedure:				
Version	**Change**	**Reason for change**	**Date**	**Name**
3.0	Version and Date	Annual Review	06/03/2014	C Burke
