Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Virtual Private Network (VPN) 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 VPN Policy Ref No. 030
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

This policy details **TfGM's** standards for site-to-site VPNs. The purpose of this policy is to specify the security standards required for such access, ensuring the integrity of data transmitted and received, and securing the VPN pathways into the network.

2 Policy Scope

a) A Virtual Private Network, or VPN, provides a method to communicate with remote sites securely over a public medium, such as the Internet.
b) A site-to-site VPN is a dependable and inexpensive substitute for a point-to-point Wide Area Network (WAN).
c) Site-to-site VPNs can be used to connect the LAN to a number of different types of networks: branch or home offices, vendors, partners, customers, etc.
d) As with any external access, these connections need to be carefully controlled through a policy.

The scope of this policy covers all site-to-site VPNs that are a part of **TfGM's** infrastructure, including both sites requiring access to **TfGM** network (inbound) and sites where **TfGM** connects to external resources (outbound). Note that remote access VPNs are covered under IS Remote Access 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

The VPN is monitored by logs on the CISCO ACS (Secure Access Control), 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 Encryption

Site-to-site VPNs must utilise strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards, such as Triple DES or AES.

6.2 Authentication

Site-to-site VPNs must utilise a strong password, pre-shared key, certificate, or other means of authentication to verify the identity the remote entity. The strongest authentication method available must be used, which can vary from product-to-product.

6.3 Implementation

a) When site-to-site VPNs are implemented, they must adhere to the policy of least access, providing access limited to only what is required for business purposes.

b) This must be enforced with a firewall or other access control that has the ability to limit access only to the ports and IP addresses required for business purposes.

c) Systems that will be accessed over the site-to-site VPN should be located in a demilitarised zone (DMZ) to segment access from **TfGM'** trusted network.

6.4 Management

TfGM must manage its own VPN gateways, meaning that a third party must not provide and manage both sides of the site-to-site VPN, unless this arrangement is covered under an outsourcing agreement.

If an existing VPN is to be changed, the changes must only be performed with the approval of the Head of IS.

6.5 Logging and Monitoring

Depending on the nature of the site-to-site VPN, the Head of IS will use their discretion as to whether additional logging and monitoring is warranted. As an example, a site-to-site VPN to a third party would likely require additional scrutiny but a VPN to a branch office of TfGM would likely not be subject to additional logging or monitoring.

6.6 Encryption Keys

Site-to-site VPNs are created with pre-shared keys. The security of these keys is critical to the security of the VPN, and by extension, the network. Encryption keys must be changed yearly.

If certificates are used instead of pre-shared keys, the certificates should expire and be re-generated after three years.

7 Enforcement

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

8 Definitions

Certificate: Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.

Demilitarised 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.

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.

Remote Access VPN: A VPN implementation at the individual user level. Used to provide remote and travelling users secure network access.

Site-to-Site VPN: A VPN implemented between two static sites, often different locations of a business.

Virtual Private Network (VPN): A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

- *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	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