Transport for Greater Manchester Policy

IS Network Security Management 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 Network Security Management Ref No. 017
Version No.	8.0	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:	Head of IS (Malcolm Lowe)		Implementation date: 31st March 2019
Date:	31st March 2019		Annual review date: 31st January 2020

Table of Contents

1 Policy Aims

To ensure the protection of information in **TfGM's** multi service network along with the protection of the supporting infrastructure.

2 Policy Scope

TfGM's multi service network, including all supporting servers, infrastructure equipment and network connections.

3 Policy Delivery

This policy will be delivered to all IS 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 Network Security Management

- The secure management of networks, which may span organisational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection.

- Additional security measures are required to protect sensitive information passing over public networks. Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

- The operational responsibility for networks lies with the Communications and Server Team, reporting directly to the Head of IS, with support available from a **TfGM** approved third party service provider. These activities must be separated from desktop computer operations and carried out by the dedicated communications team.

- Responsibility for the management of remote infrastructure equipment also belongs to the communications and server team. This equipment may include servers, routers, switches, hubs, data links, firewalls etc.

- Procedures for the management of networks and remote equipment must be approved by the Head of IS. These should be reviewed on a regular basis any changes must be formally approved. Enhanced security measures, such as encryption, should be implemented to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications.

- Proactive maintenance provisions should be applied to maintain the availability of the network services and computers connected. This may be achieved by the use of **TfGM** approved monitoring systems such as Solarwinds or Microsoft Systems Centre Operations Manager. A **TfGM** approved third party support provider will also be used as a 24 hour back up.

- Appropriate logging and monitoring should be applied to enable recording of security relevant actions. The degree of monitoring should reflect the criticality of the system.
- Where possible, alerts should be set up to report on the failures of individual services critical to the running of the system.

- Management activities should be closely co-ordinated both to optimise the service to the business and to ensure that security measures and operating procedures are consistently applied across the network infrastructure.

7 Security of Network Services

Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in house or outsourced.

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels, and management requirements, should be identified. TfGM should ensure that network service providers implement these measures.

Network services include the provision of network connections, leased data links, and managed network security solutions such as firewalls and intrusion detection systems.

These services can range from simple unmanaged bandwidth to fibre optic.
Security features of network services could be:

a) Technology applied for security of network services, such as authentication, encryption, and network connection controls
b) Technical parameters required for secured connection with the network services in accordance with the security and network connection rules.
c) Procedures for the network service usage to restrict access to network services or applications, where necessary.

8 Definitions

Authentication: A security method used to verify the identity of a user and authorise access to a system or network.

Bandwidth: or digital bandwidth, a rate of data transfer, bit rate or through put measured in bits per second.

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.

Fibre Optic: is a thin flexible, transparent fibre that acts as a waveguide, or 'light pipe' to transmit light, between the 2 ends of the fibre.

- *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	06/03/2014	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
7.0	Changed operations manager to Head of IS	Annual Review	31/03/2019	C. Styler