Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Network Control 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 Control Policy 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: Date:	Head of IS (Malcom Lowe) 31st March 2019		Implementation date: 31st March 2019 Annual review date: 31st January 2020

Table of Contents

1 Policy Aims

The purpose of this policy is to describe the steps that must be taken to ensure that IS staff connecting to **TfGM's** network are authenticated in an appropriate manner, in compliance with **TfGM** standards, and are given the appropriate level of access required to perform the duties they are carrying out at that point.

This policy specifies what constitutes appropriate use of network accounts and authentication standards.

2 Policy Scope

Consistent standards for network access and authentication are critical to **TfGM's** information security and are often required by regulations or third-party agreements.

Any IS person accessing **TfGM's** computer systems has the ability to affect the security of the network. An appropriate Network Access and Authentication Policy reduces the risk of security incidents by requiring consistent application of authentication and access standards across the network.

The scope of this policy includes all IS staff who have access to **TfGM**-owned or TfGM-provided computers or require access to the network and/or systems.

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 Network Access Control

Access to both internal and external networked services should be controlled by user authentication and hardware and software security systems.

User access to networks and network services should not compromise the security of the network services by ensuring:

a) User access to information services is controlled and applied on a principle of least privilege.
b) Appropriate authentication mechanisms are applied for users and equipment.
c) Appropriate interfaces such as firewalls are in place between the organisation's network and networks owned by other organisations, and public networks.

7 Use of Network Services

Users will only be provided with access to the services that they have been specifically authorised to use. Each user must have a unique username (user ID) and secure password – please refer to **TfGM** Password Policy document.

a) Default authorised access will allow logon to **TfGM** networked desktop PC's with limited **TfGM** network resources, such as guest access to internet.

b) Further access to services must be formally requested and authorised using the **TfGM** Serviceline user procedures – see user Access Control Policy.

c) Only **TfGM** approved devices may be connected to network ports. These must be verified to have security software installed and be virus free prior to connection.

- Only IS staff may make these connections or move equipment around between ports.

- **TfGM** laptops must only be connected using designated docking devices or pre-arranged ports. If these have been off the network for more than 4 weeks they should be security checked by Serviceline before attempting to connect to the network.
- One network port is assigned and patched in by IS staff per desk. The IP Phone is connected directly to the network port and the PC or laptop is connected to the network via the phone. Any additional ports must be formally requested on an IS service request form with business justification and management endorsement.
- No personal devices must be plugged in to network ports under any circumstances. Any rogue devices will be detected by monitoring software.

d) Remote access to external systems must only be made through **TfGM** authorised connections. Internet access will be provided via a secure filtered connection. VPN and other connections to external systems must be approved, setup and configured by IS.

Unauthorised and insecure connections to network services can affect the whole organisation. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organisation's security management and control.

8 User Authentication for External Connections

Remote access to **TfGM's** systems must be through approved connections, such as VPN or Citrix – see IS Remote Access Policy and IS VPN Policy.

Appropriate authentication methods should always be used to control access by remote users. Certificates should be used to provide secure HTTPS connection for Citrix web connections or encryption in VPN connections.

Additional authentication controls should be implemented to control access to wireless networks. In particular, special care is needed in the selection of controls for wireless networks due to the greater opportunities for undetected interception and insertion of network traffic.

Two factor authentications must be used for remote access by employees, administrators and service providers to the TVM components of the network where cardholder data is processed or stored.

9 Equipment Identification in Networks

All **TfGM** equipment should be identified by a unique **TfGM** tag number recorded on **TfGM's** central Plant Register. It should also be issued with a unique network name using a pre-defined naming system. This should distinguish types of equipment from specific locations.
Naming conventions should be consistent and be provided for;

a.) Workstations – including department/location code and Tag no.
b.) Servers – including company name, service type and number of that type.
c.) Infrastructure equipment – Company, location, and sequence number.
d.) Printers – Location/Floor, type

10 Remote Diagnostic and Configuration Port Protection

a) Physical and logical access to diagnostic and configuration ports should be controlled.

b) Where possible infrastructure and server equipment which have diagnostic and configuration ports should be housed in secure server rooms or Communications cabinets which are always locked.

c) Physical access to the port should only be granted by pre-arrangement to approved support engineers.

d) Ports, services, and similar facilities installed on computers or network systems, which are not specifically required for business functionality, should be disabled or removed.

e) Any computer systems, network systems, or communication systems which are installed with a remote diagnostic or configuration facility for use by maintenance engineers, should be secured immediately on implementation by changing system defaults to secure values known only to **TfGM**.

f) If unprotected, these diagnostic ports provide a means of unauthorised access.

11 Segregation in Networks

a) Within the **TfGM** wide area network, each remote site connected via a data link should have its own separate IP range to create a subnet.

b) Where feasible, within each subnet Groups of information services, users, and information systems should be segregated i.e. split into VLANS, with servers separated from workstations, each protected by a defined security perimeter.

c) The security perimeter implemented will be defined by the security requirements needed within the subnet and should be based on the value and classification of information stored or processed in the network.

d) Within **TfGM** VLANS network data flows should be controlled using the inbuilt routing/switching capabilities, such as access control lists.

e) A Firewall should be present at each internet connection and between any DMZ and the internal network zone.

f) The initial configuration of any **TfGM** firewall is done by **TfGM's** third party Network support provider to recommended industry standards under the instruction of the communications and server support team.

g) Any changes to the firewall configuration are subject to the **TfGM** change control procedure, where business justification for the use of all services, protocols and ports allowed must be demonstrated. For any protocols deemed to be insecure, documentation of security features must be included.

h) The configuration of TfGM's firewalls and network switches should be reviewed every six months, in segments of the network where cardholder data is processed or stored.

i) Wireless networks should be segregated from internal and private networks. Strong authentication, cryptographic methods, and frequency selection should be implemented to maintain network segregation.

j) Perimeter firewalls should be installed between any wireless networks and the cardholder data environment. These firewalls should either deny or control any traffic from the wireless environment into the cardholder data environment.

12 Network Routing Control

a) Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

b) Routing controls should be based on positive source and destination address checking mechanisms.

c) Security gateways can be used to validate source and destination addresses at internal and external network control points if proxy and/or network address translation technologies are employed.

d) Shared networks, especially those extending across organisational boundaries, may require additional routing controls. This particularly applies where networks are shared with third party users.

13 Definitions

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

Cryptographic: Modern cryptographic intersects the disciplines of computer science and electrical engineering. Applications of cryptographic include ATM cards, Computer Passwords and Electronic Passwords.

DMZ: A DMZ is a physical or logical sub network that contains and exposes organisational external services to a larger untrusted network, usually the internet. It is sometimes referred to as a perimeter network.

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.

Ticket Vending Machine (TVM): A ticket machine is a vending machine that produces tickets.

VLANS: A **virtual LAN**, commonly known as a **VLAN**, is a group of hosts with a common set of requirements that communicate as if they were attached to the same domain regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

Virtual Private Network (VPN): A secure network implemented over a 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**
3.0	Version and Date	Annual Renewal	06/03/2014	C Burke
4.0	Version and Date	Annual Renewal	30/04/2015	C Burke
5.0	Version and Date	Annual Review	31/03/2016	C Burke
6.0	Version and Date	Annual Review, new Head of IS	31/03/2017	C Burke
7.0	Version and Date	Annual Review	31/03/2018	C. Styler
8.0	Version and Date	Annual Review	31/03/2019	C. Styler