Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Physical Security 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 Physical Security Policy Ref No. 020
Version No.	7.0	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

The purpose of this policy is to protect TfGM's physical information systems by setting standards for secure operations.

2 Policy Scope

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on the physical network infrastructure. In order to secure data the security of the physical Information Systems (IS) resources must be assessed to ensure that they are protected from standard risks.

The policy applies to the physical security of TfGM's information systems, including, but not limited to, all TfGM-owned or TfGM-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting TfGM's office is covered by this policy.

Please note that this policy covers the physical security of TfGM's Information Technology Infrastructure, and does not cover the security of non-IS items or employee security.

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

Security standards are in place to secure **TfGM's** operations, the standards are accessed on a regular basis to ensure all operations are protected, should a breach of policy be identified, it may be used in disciplinary proceedings.

6 Policy

6.1 Physical Security Perimeters

6.1.1 Internal Perimeter

Any area containing TfGM devices or Systems shall be considered inside the internal Perimeter.

The internal perimeter shall be subject to access controls to guard against unauthorised access.

General TfGM employee offices will be controlled by card reader devices on all floors internally except the 1st floor meeting room area.

Private offices will be controlled by lock and key

CCTV cameras and card reader devices will be used to monitor individual physical access to sensitive areas, such as server rooms, control rooms or storage rooms. These rooms must be restricted to personnel who have a business requirement to enter. All other access must be necessary, authorised and recorded in the visitor's book. Access to such areas must be reviewed on a regular basis.

6.1.2 External Perimeter Entry/Exit Points

CCTV Cameras must be placed within the external perimeter to record the entry/exit points, in a position to record in detail sufficient to later identify the person who gained access.

Barriers must be present to restrict access from the public reception area to TfGM internal offices.

Reception desk must be manned at all times and access to the internal area will be granted to visitors, only if they have been notified in advance and escorted by a member of staff.

The underground car park/loading bay entrance must be kept closed at all times and access controlled by reception staff.

A professionally monitored security alarm system must be used to minimise risk of theft, or reduce loss in the event of a theft. The system must be monitored 24x7, with TFGM personnel being notified if an alarm is tripped at any time.

6.1.3 Public Access Areas

Public access will be restricted to the reception waiting area. Outside core hours, the front door will be set to exit only and must be locked when reception is not manned.

6.1.4 Central Server System Security

TfGM must ensure that central server facilities only have physical entry points from within the building housing them. Provide secure points of entry to the server room, to secure sensitive data, limit the possibility of employee vandalism, minimise exposure to inappropriate psychometric or contaminant conditions, and control the possibility of failures caused by inadvertent actions of untrained personnel.

6.1.5 Terminal and Console Security

When not in use, all devices contained within the internal and external perimeters must have any console access locked to prevent unauthorised use.

6.2 Access Controls

Access controls are necessary to restrict entry to TfGM's premises and security zones to only approved persons. There are a several standard ways to do this, which are outlined in this section, along with the guidelines for their use.

6.2.1 Keys and Keypads

Keys and keypads may be used in areas where access is limited. Keys must be marked "do not duplicate" and their distribution must be limited and recorded. Keypad users must take care to ensure that keypad codes are not shared unnecessarily or seen during input. If it is suspected that the key or code has been lost or compromised, the locks or codes must be changed immediately. They should also be used in conjunction with another security strategy, such as an alarm system or CCTV.

6.2.2 Key Cards

The use of key cards is the preferred option for TfGM Internal and external access control. Key cards will be configured to set access unique to the individual user and to forbid access to security zones where they are not authorised. Schedules may be set to forbid off-hours access. If a key card is lost or stolen it must be immediately disabled. If an employee is terminated or resigns, that user's access must be disabled. When issuing replacement key cards the old key card must be either disabled or destroyed.

6.3 Entry Security

It is the policy to provide a safe workplace for employees. Monitoring those who enter and exit the premises is a good security practice in general, but is particularly true for minimising risk to systems and data. The guidelines below are specific to the information technology assets.

6.3.1 Use of Identification Badges

Identification badges are useful to identify authorised persons on TFGM's premises. The following guidelines must be used for the use of ID badges.

- Employees: ID badges are required.
- Non-employees/Visitors: At generic Visitor badge is required.

6.3.2 Sign-in Requirements

A sign-in log must be maintained (or similar device) in the lobby or entry area and visitors are required to sign in upon arrival. At minimum, the register must include the following information:

- visitor's name
- company name
- reason for visit
- name of person visiting
- sign-in time
- sign-out time

6.3.3 Visitor Access

Visitors should be given only the level of access to TfGM' premises that is appropriate to the reason for their visit.

After checking in, visitors must be escorted unless they are considered "trusted" by TfGM.

Examples of trusted visitor's may include TfGM's legal counsel, financial advisor, or a consultant that frequents the office, and will be decided on a case-by-case basis.

6.4 Equipment Siting

6.4.1 Locating Data Centres

The Data Centre must be located in a suitable position to avoid risk from damage from many sources.

Below building grade must be avoided, due to leakage potential. Lower floors are unsuitable due to possibility of break-in through external windows.

The Data Centre must be located in an area that offers the potential for future expansion. Even though technology changes tend to make hardware more space-efficient over time, the ability to expand, either within the current footprint of the building, or through additions, should be available to accommodate possible growth as the room evolves.

Ensure adequate access is allowed to handle equipment movement in, out and within the data centre, with adequate space for maintenance or replacement of large equipment such as air conditioning units. This will include appropriate door sizes negotiable corners, ramps and smooth floor surfaces.

The raised floor space, air conditioning support, uninterruptable power supply (UPS), generators, and related support equipment must be coordinated with other areas of the building and properly positioned within the building perimeter in order to optimise their interaction and the overall support of operations.

6.4.2 Equipment Safeguards

Isolate the computer room from contaminant producing activities, such as print rooms or kitchens.

Ensure the exhaust from generators or other sources does not directly enter the intake of air handlers serving the computer room.

Do not locate the data centre beneath kitchens, workshops, or other areas that have a high potential for leaks. Avoid locating the hardware areas beneath potential liquid leaks.

Do not run the air conditioner piping through the ceiling void of the computer room.

Ensure the perimeters are sealed, as expansion joints, conduit or pipe penetrations, cracks and other breaches can all allow for water infiltration.

Design the raised floor computer spaces in convenient proximity to the support equipment (UPS, chillers, etc.). It is often appropriate to locate the data centre on floors above the support equipment in order to consolidate cooling and power trunk lines.

6.5 Power Supplies

Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for all Server and Network hardware or Workstations that are located in areas susceptible to power surges. These devices must carry a warranty that covers the value of the systems if the systems were to be damaged by a power surge.

6.6 Cabling and Communications Equipment

Network cabling must not run through non-secured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).

Network ports that are not in use must be disabled.

6.7 Equipment Maintenance

Equipment maintenance should only be carried out by qualified Engineers

6.8 Off Site Equipment

Mobile equipment such as Laptops, IPads & mobile phones must be encrypted where possible, or protected with a pin code.

Laptop locks and cables must be used to secure laptops when left in the office or other fixed locations. Alternatively a laptop can be locked away in a secure drawer or cabinet.

Mobile devices should be kept out of sight when not in use.

Care should be given when using or transporting mobile devices in busy areas.

Mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the car boot, with the interior boot release locked; or in a lockable compartment such as a glove box.

For all mobile devices connected to the TfGM network and where practical a remote wipe/remote delete technology must be implemented.

6.9 Disposal and re-use of equipment

Equipment which has reached end of life must be securely disposed according to WEEE standards. Any disks holding data on should be securely erased or destroyed, so as data cannot be retrieved at a later date.

Equipment which can be re-used, must be re-imaged to ensure that there is no residual data from the previous user.

6.10 General Equipment Security

Precautions must be taken to ensure the integrity of **TfGM's** equipment and data. At a minimum, the following guidelines must be followed:

- Computer screens must be positioned where information on the screens cannot be seen by outsiders.
- Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorised to view the information.
- Users must lock their workstations whenever they leave the workstation unattended.
- Users must logoff or shut down their workstations when leaving for an extended time period.
- Users must shut down their workstations prior to leaving the office.
- Users must shutdown their workstations at the end of the workday.

6.11 Minimising Risk of Loss and Theft

In order to minimise the risk of data loss through loss or theft of company property, the following guidelines must be followed:

- **Unused systems:** If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured.
- **Mobile Devices:** Special precautions must be taken to prevent loss or theft of mobile devices. Refer to the Mobile Device Policy for guidance.
- **Systems that store confidential data:** Special precautions must be taken to prevent loss or theft of these systems. Refer to the Confidential Data Policy for guidance.

6.12 Minimising Risk of Damage

Systems that store data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimise the risk of damage, the following guidelines must be followed:

1. Environmental controls must keep the operating environment of systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.
2. Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimised.
3. Strong magnets must not be used in proximity to systems or media.
4. Except in the case of a fire suppression system, open liquids must not be located above company systems. Technicians working on or near systems should never use the systems as tables for beverages.
5. Beverages must never be placed where they can be spilled onto systems.

6.13 Fire Prevention

It is **TfGM's** policy to provide a safe workplace that minimises the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IS systems, the fire danger in these areas is typically higher than other areas of the office. The following points must be adhered to and conform to overall fire safety policy:

1. Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.
2. Electrical outlets must not be overloaded. Users must not chain multiple

power strips, extension cords, or surge protectors together.

3. Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.
4. Only electrical equipment that has been approved by Underwriters Laboratories and bears the UL seal of approval must be used.
5. Unused electrical equipment must be turned off when not in use for extended periods of time (i.e., during non-business hours).
6. Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly-worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.
7. A fire alarm monitoring service must be used that will alert a designated employee if an alarm is tripped during non-business hours.

6.14 Malicious Attack and Accidental Damage

Malicious threats consist of internal attacks by disgruntled or malicious employees and external attacks by non-employees who are looking to harm or disrupt an organization.

Accidental damage can be caused by internal staff, who are not aware of the actions they are taking, often un-intentional errors which destroy data, or introduce security risks. Other external threats may consist of events where external damage may be caused to the building by out of control cars or derailed trams.

Controls to minimise or deter Malicious Attack's or accidental damage must include:-

1. Limit entry points to the building, to reduce the points of attack
2. Control access to the parking area
3. Make fire doors exit only, with no handles on the outside. These doors should be alarmed.
4. Use plenty of cameras to deter attack and record any events.
5. Use landscaping for protection, to prevent direct vehicular access to the front of the building.
6. Implement strong acceptable use policies, with clear penalties for non-adherence, and ensure adequate monitoring is enforced.

6.15 Natural Disasters

It is impossible to prevent Natural Disasters, therefore the best approach is to have disaster recovery plans and contingency plans in place. Earthquakes, hurricanes, floods, and lightning can cause severe damage to computer systems, causing downtime or loss of productivity, disrupting essential services. Information can be lost or destroyed.

A few safeguards must be implemented against natural disasters.

1. Ensure any computer equipment is positioned above any expected flood levels, where possible. The data centre should be positioned a couple of floors above the ground.

2. Ensure disaster recovery plans are developed and kept up to date.

3. Develop procedures to shut down equipment in the event that the facility must be evacuated for a prolonged period of time where it is not safe to keep the equipment running

4. Develop a removal plan for IT Assets in the event that the building is damaged to the point where it cannot be utilised.

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

Datacentre: A location used to house a company's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.

Key card: A plastic card that is swiped, or contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.

Keypad: A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.

Mobile Device: A portable device that can be used for certain applications and data storage. Examples are PDA's or Smartphones.

PDA: Stands for Personal Digital Assistant. A portable device that stores and organises personal information, such as contact information, calendar, and notes.

Smartphone: A mobile telephone that offers additional applications, such as PDA functions and email.

Uninterruptible Power Supplies (UPS's): A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically also contains power surge protection.

- *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
3.1	Added sections – Natural Disaster, Malicious Attack & Fire	After P&P Audit	31/05/2015	J Singleton
4.0	Version and Date	Annual Review	31/03/2016	C Burke
5.0	Version and Date	Annual Review, new Head of IS	31/03/2017	C Burke
6.0	Version and Date	Annual Review	31/03/2018	C Styler
7.0	Version and Date	Annual Review	31/03/2019	C Styler