Transport for Greater Manchester

Transport for Greater Manchester Policy

003 IS Asset Management Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31st March 2020	Document Reference no.	IS Asset Management Policy Ref No. 003
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:	Malcolm Lowe (Head of IS)		Implementation date: 31st March 2020 Annual review date: 31st January 2021

Table of Contents

1 Policy Aims

To identify TfGM information and information processing assets and define appropriate protection responsibilities, hereby known as TfGM assets within this policy.

2 Policy Scope

This policy covers all TfGM assets associated with information and information processing facilities.

3 Policy Delivery

The 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; Information Asset Owners responsible for compliance with information asset register actions.
- Awareness: All

5 Policy Monitoring/ Compliance

All departmental managers are responsible for ensuring compliance with identified legal requirements and security procedures within their department.

Bi-annually reviews will be undertaken by Serviceline, who will circulate the asset register to departmental managers. Departmental managers must advise the list is up-to-date and ensure compliance within this policy.

Should a breach of this policy be identified, it may be used in disciplinary proceedings.

6 Policy

6.1 Responsibility for Assets

Departmental Managers and IS Asset owners have responsibility to ensure adequate security of all TfGM's assets. These must be identified and appropriate protection defined. The responsibility for each TfGM asset rests with assigned owner who will notify IS of any changes to ownership or transfer of assets.

6.1.1 Inventory of Assets

All TfGM assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained, including updates of changes by Departmental Managers and IS Asset owners.
The process of compiling an inventory of assets is an important prerequisite of TfGM's risk management approach.

Assets include

- Hardware
- Software
- New Acquisition and Changes

IS asset systems in use at TfGM include:

- Plant Register, this contains all hardware assets associated with information processing, such as PC's, servers, monitors, communications equipment etc, and is reviewed on an annual basis.
- Snow Asset Management (SAM) is used to store all Software Assets, such as licenses, maintenance agreements and software license audit data, and is reviewed on an annual basis.
- Vodafone Corporate Online (VCOL) system is used to manage TfGM's company mobile phones and services, billing. Order of new devices, manage SIMs and connections, track orders and monitor usage, and is reviewed on renew of contract.
- MSN Asset Register contains a log of all Multi Service Network devices, this register is reviewed in line with a technology refresh.

Hardware asset registers (Plant Register) should be maintained at every stage in the equipment lifecycle, including;

- Procurement
- Deployment
- Management (equipment movement)
- Disposal

They should include the following information

- location
- type (make, model, configuration)
- supplier **THIS IS NOT INCLUDED ON OUR EXCEL SPREADSHEET**
- replacement value – i.e., net present value at procurement or purchase
- serial number

Software Asset Registers (Needs revision from the Access Database used at present) should be maintained at every stage in the Software asset management lifecycle;

- Request/Approval/Stock check
- Procurement
- Deployment/re-deployment of unused software/upgrade
- Maintenance
- Disposal

They should include the following information

- Supplier **(NOT INCLUDED AT PRESENT) FOR HARDWARE)**
- Version
- Maintenance details
- Serial number
- No of licenses
- Type of license

Vodafone Corporate Online Systems should be maintained at every stage in the asset management lifecycle;

- Request/Approval/Stock check
- Procurement
- Deployment/re-deployment
- Maintenance
- Disposal

They should include the following information

- IMEI Number
- SIM Number
- Subscriber Name
- Contact Type
- Manufacturer
- Model

MSN Asset Register should be maintained at every stage in the asset management lifecycle;

- Request/Approval/Stock check
- Procurement
- Deployment/re-deployment
- Maintenance

- Disposal

They should include the following information

- Supplier/Vendor **(NOT INCLUDED AT PRESENT) FOR HARDWARE)**
- Product Description
- Component ID
- Serial number
- Tag No

Inventories of assets help to ensure that effective protection takes place, and may also be required for other purposes, such as health and safety, insurance or financial (asset management) reasons.

6.1.2 Ownership of Assets

All TfGM assets maintained in the inventories should be assigned an owner. The owner may be an individual, job role, team or department. The identified owner does not necessarily have any property rights to the asset.

Ownership should be assigned when assets are created or when assets are transferred to the organization. The asset owner should be responsible for the proper management of an asset over the whole asset lifecycle.

The asset owner should:

- ensure that assets are inventoried
- ensure that assets are appropriately classified and protected
- define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies
- Ensure proper handling when the asset is deleted or destroyed.

Routine tasks may be delegated, e.g. to a custodian looking after the assets on a daily basis, but the responsibility remains with the owner.
In complex information systems, it may be useful to designate groups of assets which act together to provide a particular service. In this case the owner of this service is accountable for the delivery of the service, including the operation of its assets.

6.1.3 Acceptable use of assets

The acceptable use of TfGM information and information processing assets is documented in the IS Acceptable use Policy, IS Mobile Device Usage Policy, and the Data Protection Policy. TfGM users should ensure that they are familiar with these policies.

Employees and external party users using or having access to the organisation's assets should be made aware of the information security requirements of the organisation's assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

Any use of TfGM IS and information facilities for non-business or unauthorised purposes, without prior management approval, will be regarded as improper use of the facilities and may lead to disciplinary action.

6.1.4 Return of assets

All employees and external party users must return all of the TfGM assets in their possession upon termination of their employment, contract or agreement.

The termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to TfGM.
In cases where an employee or external party user purchases the organization's equipment or uses their own personal equipment, all relevant information must be transferred to TfGM and securely erased from the equipment.
In cases where an employee or external party user has knowledge that is important to ongoing operations, that information should be documented and transferred to TfGM.

During the notice period of termination, unauthorised copying of relevant information (e.g. intellectual property) by terminated employees and contractors is strictly forbidden.

6.2 Information classification

Information classification is used to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

6.2.1 Handling of assets

Handling of Software and Hardware Assets can be found in the Information Services Asset Recording Procedure. Refer to ;

- PR03 –(IS) Information Asset Recording Procedure
- PR08 – (IS) Information Services Asset Disposal Procedure.

(NOT SURE WHAT/WHERE THIS IS – WILL CHECK WITH CATH BURKE)

6.3 Media Handling

Media handling controls are essential to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.
See 021 IS Removable Media Policy for a full description of TfGM's policy for the use of removable media for TfGM users.

6.3.1 Management of removable media

The following policies for the management of removable media should be adhered to

- When no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable.
- When necessary for business purposes, authorisation will be required for media removed from TfGM and a record of such removals should be kept in order to maintain an audit trail.
- All media should be stored in a safe, secure environment, in accordance with manufacturers' specifications.
- For all TfGM data in transit, cryptographic techniques should be used to protect data on removable media.
- To mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh media before becoming unreadable
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of coincidental data damage or loss.
- A record of removable media issued will be maintained to limit the opportunity for data loss.
- Removable media drives should only be enabled if there is a business reason for doing so
- Where there is a need to use removable media the transfer of information to such media should be monitored.

6.3.2 Disposal of media

Media should be disposed of securely when no longer required, using TfGM secure disposal procedures.

The following policies must be observed:

- Media containing confidential information must be securely disposed, e.g. by incineration or shredding, or erasure of data for use by another application within TfGM. It may be easier to arrange for all media items to

be collected and disposed of securely, rather than attempting to separate out the sensitive items.

- A suitable external party with adequate controls and experience should be selected if appropriate;
- Sensitive items disposed of should be logged in order to maintain an audit trail.
- When accumulating media for disposal, consideration should be given to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.
- Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.

6.3.3 Physical media transfer

TfGM media containing information should be protected against unauthorized access, misuse or corruption during transportation. In order to achieve this, the following policies should be followed:

- Reliable transport or couriers should be used.
- A list of authorized couriers should be agreed with management.
- Procedures to verify the identification of couriers should be followed.
- Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields.
- Logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media, including paper documents, via the postal service or via courier.
When confidential information on media is not encrypted, additional physical protection of the media should be considered.

7 Enforcement

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

b) Any equipment identified as stolen will be handled within the scope of Corporate Asset Recovery and Sanctions Policy, please refer to the Theft Response Policy.

8 Glossary and References

8.1 References

- PR03 –(IS) Information Asset Recording Procedure
- PR08 – (IS) Information Services Asset Disposal Procedure.
- Theft Response Policy

Change control record: complete each time there is a change

Policy/Procedure:				
Version	**Change**	**Reason for change**	**Date**	**Name**
1.1	review	Changes to draft by Michelle Peel accepted by Jude Singleton	24/07/15	Jude Singleton
2.0	Date & Version	Annual Review	31/03/2016	C. Burke
3.0	Date & Version	Annual Review and Head of IS Change.	31/03/2017	C. Burke
4.0	Review	Changes of Improvement made from audit recommendations.	27/09/2017	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
7.0	Review	Pre-Annual Review check	09/01/20	K. Murray