Transport for Greater Manchester

Transport for Greater Manchester Policy

# Human Resources Information 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 Policy Ref no. |
| Version No. | 10.0 | Prepared by: | Ian Elwers |
| Equality Impact Assessment | Validation of Initial Screening<br><br>Equality Officer: Muhammad Karim<br><br>**Date:** | | Full Impact Assessment completed:<br>YES<br><br>**Validated by Equality Officer signature:**<br><br>**Date:** |
| | If any changes are made to this document, its impact upon legally protected groups will need to be re- assessed. Please underline one of the options below that is most appropriate:<br>1. No change or minor changes - EQIA not required<br>2. Some changes - Initial Screening Completed | | |
| Authorisation Level required: | Executive Group/Director | | Staff Applicable to:<br><br>All Staff |
| Authorised by:<br><br>Date: | Head of IS (Malcolm Lowe)/Director of HR (David Alexander)<br><br>31st March 2019 | | Implementation date:<br><br>31st March 2019 |
| | | | Latest review date:<br><br>31st January 2020 |

## 1 Policy Aims

a) Transport for Greater Manchester (TfGM) is committed to protecting itself and:
   - its employees;
   - others engaged to provide its services; and
   - its partners;

   from illegal or damaging actions by others.

a) TfGM will therefore ensure that users of information systems:
   - understand their responsibilities regarding access to and use of our information systems and the information they contain;
   - sign to indicate that they understand and will abide by their responsibilities regarding information systems;
   - are trained to use information systems securely.

b) TfGM will also ensure that:
   - any checks deemed appropriate are carried out on users prior to allowing them access to information systems;
   - a user's access to information systems is removed promptly when the requirement for access ends.

## 2 Review and Update of the Policy Statement

a) This Policy is reviewed at least annually by **TfGM's HR and IS Teams** to ensure:
   - appropriate secure use of information systems including, but not limited to, computer systems, email, internet and network access;
   - appropriate checks are carried out prior to allowing information system access;
   - appropriate training is undertaken.

## 3 Purpose

a) TfGM legitimately holds a large amount of personal and business-sensitive information. We recognise that technical solutions alone cannot ensure absolute confidentiality and security of this information.

b) This policy therefore addresses the security issues that relate to users of our information systems in order to afford protection as detailed in 1 a) above.

## 4 Scope

a) This policy applies to individuals who have access to our information systems and/or use the information contained within them (known as 'users' of these systems) Users may be:

- employees;
- agency workers;
- contractors;
- employees seconded to TfGM;
- delivery partners;
- Board Members; and
- anyone else who is authorised to access information systems on behalf of TfGM.

## 5 Policy Delivery

a) This policy will be delivered by internal communication and will be situated on the TfGM Intranet.

## 6 Accountability

a) Responsible to the Board: Heads of IS and HR
b) Compliance: Managers to ensure that their direct reports comply with this policy
c) Awareness: All Staff

## 7 Monitoring/Compliance

a) Information including logon dates, times, usage duration and device identity will be logged and may be used for monitoring purposes, and disciplinary proceedings.

b) The application of pre-employment/engagement screening will be routinely monitored.

c) Failure to abide by the responsibilities regarding information systems will be investigated in accordance with the Disciplinary Policy where users are employed directly. Action appropriate to the circumstances will be taken where the user is not directly employed by TfGM.

d) In extreme circumstances, Audit & Assurance may access equipment or information to help support investigations.

## 8 Policy Application

8.1 Prior to employment/engagement – roles and responsibilities

Individuals are required to adhere to TfGM policies and procedures in accordance with their terms and conditions of employment or terms of their engagement. Security responsibilities will be included in appropriate role profiles.

8.2 Prior to employment/engagement – screening

a) All candidates for direct employment will be recruited in accordance with TfGM's Recruitment Policy and Procedure. Appointment is conditional on:
- satisfactory checks on the individual's right to work in the UK;
- reference(s) covering the last 3 years of employment;
- confirmation of claimed academic and professional qualifications, where these are a requirement of appointment;
- complete health questionnaire for occupational health screening

b) HR will ensure that the above checks are carried out.

c) The same requirements apply to:
- agency workers (screening undertaken by agency);
- contractors (screening undertaken by supplying organisation);
- employees seconded to TfGM (screening undertaken by substantive employer);
- anyone else who is authorised to access information systems on behalf of TfGM.

d) If recruitment agencies/consultancies are used to provide candidates for potential employment by TfGM, their responsibility for appropriate screening will be specified to them by HR before appointment.

e) This also applies where recruitment agencies/consultancies are used to provide agency workers or consultants (i.e. individuals who will be engaged TfGM, rather than directly employed)

f) HR will specify the requirements for screening to self-employed contractors; and to the employers of secondees/delivery partners prior to engagement.

g) TfGM uses specialist recruitment consultants to recruit Board Members who are not directly employed. Consultants are advised of their responsibility for appropriate candidate screening.

8.3 Prior to employment/engagement - access to information systems

a) The line manager is responsible for identifying access requirements to information systems appropriate to the user's role. In accordance with the IS Access Control Policy, the line manager must:
   - complete a Service Request Form and submit it to Serviceline;
   - complete a Request to Recruit Form and submit it to HR.

b) When the Service Request Form has been received; and when the Request to Recruit Form has been processed, access will be arranged.

8.4 On commencement of employment/engagement

8.4.1 Corporate induction

a) All individuals employed or engaged (i.e. when they are not directly employed) by TfGM must complete the corporate eLearning induction within their first week. This includes the following elements:
   - indicating their acceptance of IS policies via the Learning Portal on the intranet;
   - indicating their acceptance of TfGM's confidentiality agreement;
   - completing a local induction checklist to confirm that all necessary information has been provided. As part of their local induction, individuals will be advised of any security responsibilities. If the individual has access to systems processing payment card data, appropriate training as required by the Payment Card Industry Data Security Standards (PCI-DSS) will form part of their local induction.

b) Individuals cannot complete their induction until they have completed all the elements above. Records of completion will be stored electronically on each individual's personal file.

### 8.4.2 Compliance eLearning

a) During an agreed timescale, all individuals employed or engaged must complete compliance eLearning to ensure their understanding of and compliance with TfGM's requirements in relation to all mandatory eLearning as detailed in the Learning Portal.

b) This requires the individual to:
   - complete a series of learning modules to ensure they understand TfGM's requirements; and/or (where applicable)
   - complete declarations that they will abide by these requirements

c) Records of completion will be stored electronically on the individual's personal file.

### 8.4.3 Probationary period

a) Employees are subject to a 6 month probationary period, during which their suitability for their role and compliance with information security responsibilities will be regularly assessed by their line manager. Employees will remain on probation and will not be confirmed in post until mandatory eLearning is completed.

### 8.4.4 Training

a) The line manager must ensure that:
   - users receive adequate training promptly in order to use information systems appropriately, efficiently and securely;
   - users receive refresher training where necessary (e.g. following maternity/shared parental leave or long term sick leave);
   - user training is updated when updates are made to systems, or when systems are replaced.

## 8.5 Ongoing requirements

a) When IS policies are revised, or new policies are introduced, all users must read them and complete a further declaration via eLearning to indicate their understanding and compliance with the policies. Declarations will be stored on the user's personal file.

b) Compliance eLearning will be repeated as stipulated in the appropriate module, or when the requirements of statute or those of TfGM change.

### 8.6 Changes in role

a) In accordance with the IS Access Control Policy, the line manager must:
   - Update the SAP HR system;
   - notify HR promptly when a user is given a new role; or where there are changes in a user's existing role which entail changes to their access to or usage of information systems. This is to ensure that access to systems can be changed as appropriate, including removing access where this is no longer required.

b) Serviceline will be automatically informed of the changes.

c) If the user has access to systems processing payment card data as a result of these changes, they must receive appropriate training as required by the Payment Card Industry Data Security Standards (PCI-DSS).

d) The line manager must ensure that any training requirements arising from a new job or changes in their existing job are carried out promptly and adequately.

### 8.7 Termination of employment/engagement

#### 8.7.1 Notification of termination

a) In accordance with the IS Access Control Policy, the line manager must:
   - update the SAP HR system;
   - notify HR of the termination of a user's employment/engagement so that access to information systems can be removed at the appropriate time.

b) Serviceline will be automatically informed of the termination.

c) The line manager must also notify HR promptly if a user is suspended from duty so that access to information systems can be removed for the duration of the suspension.

#### 8.7.2 Return of assets

a) The line manager is responsible for ensuring that all passes, mobile phones, lap top computers, tablets, USB sticks, CDs/DVDs, rail passes, tram/bus passes and keys as appropriate; and copies of information in any format belonging to TfGM are returned by individuals on termination of employment/engagement.

b) The line manager must ensure that returned items are delivered to the appropriate departments of TfGM promptly.

## 8.8 Relevant policies

a) This policy should be read in conjunction with:
   - all IS and PCIDSS policies which are available on the intranet under work areas/IS/information systems/information services/shared documents;
   - the Data Protection Policy;
   - the following HR policies which are available on the intranet under work areas/Human Resources/HR Policies and Procedures:
     - Code of Conduct;
     - Disciplinary Policy;
     - Recruitment and Selection Policy.