MAYOR OF LONDON

Agreement Reference Number: ITC10686

Date:

Framework Agreement
for the Provision of Wireless Communications including Voice, Data, Associated Airtime Accessories & Services

between

Transport for London

and

Telefónica O2 UK Limited

TABLE OF CONTENTS

THIS AGREEMENT is made the day of 2009

BETWEEN:

(1) **Transport for London a** statutory corporation whose principal office is at Windsor House, 42-50 Victoria Street, London, SW1H 0TL (**"TfL"**); and

(2) **Telefónica 02 UK Limited**, a company registered in England and Wales (Company Registration Number 01743099) whose registered office is at 260 Bath Road, Slough, Berkshire, SL1 4DX ("**the Service Provider"**).

RECITALS:

A. The Parties wish to enter into a framework agreement which will enable TfL, from time to time, to contract with the Service Provider on a call off basis ("a call-off" Contract) for some or all of the Products and Services of the type described in Schedule 3.

B. The terms and conditions of this Agreement shall apply to the Products and Services to be provided by the Service Provider under any Call-Off Contract.

C. This framework agreement can be utilised by TfL or any other member of the TfL Group.

D. The terms and conditions of this Agreement provide that the Greater London Authority or any of its other functional or associated bodies may contract with the Service Provider on the terms set out in this Agreement for the procurement of the Products and Services.

THE PARTIES AGREE THAT:

In consideration of the payment by TfL to the Service Provider of £5.00 (the receipt and sufficiency of which is acknowledged by the Service Provider) and the mutual promises and covenants set out in this Agreement, the Parties agree as follows:

1. DEFINITIONS AND INTERPRETATIONS

In the Agreement (including the Recitals):

1.1 unless the context indicates otherwise the following expressions shall have the following meanings:

"Agreement"	this framework agreement, including the Schedules and all other documents referred to in this Agreement;
"Agreement Commencement Date"	the date for commencement of this Agreement specified in Schedule 1;

"Agreement Reference Number"	the reference number for this Agreement as set out in Schedule 1;
"Bespoke Products and/or Services"	any products, services, documents, drawings, software or other work developed or prepared by or on behalf of the Service Provider which the Parties agree are developed specifically for TfL or in accordance with TfL's requirements for agreed monetary consideration and are not to be used by the Service Provider for its other customers or generically in its business and exclude for the avoidance of doubt the Products and Services detailed in Schedule 3;
"Business Day"	any day excluding Saturdays, Sundays or public or bank holidays in England;
"Business Continuity"	the plan that the Service Provider will comply with when responding to a Disaster, details of which are set out in Schedule 11;
"Call-Off Contract"	a call-off contract in the form of the Delivery Request Form which has been acknowledged by the Service Provider for the provision of the Services which incorporates this Agreement and includes any attachments and any documents expressly referred to in that Call-Off Contract;
"Call-Off Contract Number"	the reference number for a Call-Off Contract, as specified in the relevant Delivery Request Form;
"Call-Off Co-ordinator"	the person named as such in a Call-Off Contract or such other person as notified to the Service Provider by TfL;
"Call-Off Term"	the duration of a Call-Off Contract, as set out in the relevant Delivery Request Form or as specified in Schedule 3;
"Charges"	the charges payable by TfL, in consideration of the supply of the Products and the due performance of the Services as set out in Schedule 6 , and as applicable to each Call-Off Contract;

"Confidential Information"	in relation to a Party, all information (whether written or oral) that by its nature may reasonably be regarded as confidential to that Party or any other member of that Party's Group (whether commercial, financial, technical or otherwise) including information which relates to the business affairs, customers, suppliers, products, software, telecommunications, networks, trade secrets, know-how or personnel of that Party or any member of that Party's Group;
"Delivery Address"	means the address where the Products are to be delivered, as specified in the relevant Delivery Request Form (and if more than one address is specified in relation to different Products, then the relevant address for delivery);
"Delivery Date"	means such date as is specified in the relevant Delivery Request Form (and if more than one date is specified in relation to different Products, then the relevant date for delivery) or if no such date is specified then not less than 4 Business Days after the date of the relevant Delivery Request Form;
"Delivery Request Form"	a document produced by TfL pursuant to clause 3, setting out its requirements for the Products / Services from the Service Provider, which document, by way of example only, shall substantially be in the form set out in Schedule 7 or in such other form as may be notified to the Service Provider by TfL from time to time;
"Disaster"	any unplanned interruption or event which significantly impairs (i) the ability of the Service Provider to perform the Services or (ii) the ability of TfL or the TfL Group to receive the Services (in whole or in part) in accordance with the terms of this Agreement;
"Euro Compliant"	means that the Products are capable of supporting the Euro (if applicable) and will not manifest any material error nor suffer a diminution in performance or loss of functionality as a result of the introduction of the Euro as a currency in certain EU member

	states and the Products shall (if applicable) be capable of processing transactions calculated in Euros separately from or in conjunction with other currencies and shall be capable of complying with any legislative changes relating to the Euro;
"Force Majeure Event"	any of the following: riot, civil unrest, war, act of terrorism, threat or perceived threat of act of terrorism, fire, earthquake, extraordinary storm, flood, abnormal weather conditions or other natural catastrophe or strikes, lock-outs or other industrial disputes to the extent that such event has materially affected the ability of the Party relying on the Force Majeure Event ("Affected Party") to perform its obligations in accordance with the terms of this Agreement but excluding any such event insofar as it arises from or is attributable to the wilful act, omission or negligence of the Affected Party or the failure on the part of the Affected Party to take reasonable precautions to prevent such Force Majeure Event or its impact;
"GLA Bodies"	means the Greater London Authority, its functional bodies (as may change from time to time but, at the date of this Agreement the Metropolitan Police Authority, the London Development Agency and the London Fire and Emergency Planning Authority), and associated bodies.
"Holding Company"	any company which from time to time directly or indirectly controls the Service Provider where "control" is as defined by section 840 of the Income and Corporation Taxes Act 1988;
"Insolvency Event"	any of the following: (a) the Service Provider and/or the Holding Company making any voluntary arrangement with its creditors or becoming subject to an administration order; (b) a receiver, administrative receiver, manager, or administrator being appointed over all or part of the business of the Service Provider and/or the Holding Company;

	(c) being a company, the Service Provider and/or the Holding Company having passed a resolution for its winding-up or being subject to a petition for its winding-up (except for the purposes of a voluntary amalgamation, reconstruction or other re-organisation without insolvency); (d) the Service Provider and/or the Holding Company ceasing or threatening to cease to carry on its business for any reason and/or being unable to pay its debts within the meaning of the Insolvency Act 1986; (e) being an individual or firm, the Service Provider becoming bankrupt or dying; (f) any similar event to those in (a) to (e) above occurring in relation to the Service Provider and/or the Holding Company under the law of any applicable jurisdiction for those purposes;
"Intellectual Property Rights"	any patent, know-how, trade mark or name, service mark, design right (in each case whether registered or unregistered), copyright, rights in passing off, database right, rights in commercial or technical information, any other rights in any invention, discovery or process and any other intellectual property rights, whether registered or unregistered and including applications for the grant of any such rights and all rights or forms of protection having equivalent or similar effect in each case in the United Kingdom and anywhere else in the world;
"Key Personnel"	the Service Provider's key personnel named as such in Schedule 1 or any relevant Call-Off Contract;
"Direct Losses"	all costs (including legal costs and costs of enforcement), expenses, liabilities (including any tax liability), injuries, and direct loss, which includes without limitation pure economic loss, loss of business, depletion of goodwill and like loss but excludes loss of profits and loss of anticipated savings

	(whether direct or indirect) and any indirect or consequential loss), damages, claims, demands, proceedings and judgments;
"Milestone"	an event which is the completion of one or more of the specified activities as may be set out in the Project Plan;
"Parties"	TfL and the Service Provider (including their successors and permitted assignees) and "Party" shall mean either of them as the case may be;
"Products"	means all or any part of the products to be supplied by the Service Provider as detailed in Schedule 3 and the Technical Requirements Specification and which shall be included under a Call-Off Contract;
"Project Plan"	the plan (if any) set out in a Call-Off Contract in relation to the performance and timing of the Services under a Call-Off Contract which may include Milestones;
"Procurement Manager"	the person named as such in Schedule 1 or such other person as notified to the Service Provider by TfL;
"Required Date"	the date or dates on or by which each Milestone is required to be completed as set out in the Project Plan (if any) or, in the absence of any Milestones, the date or dates on or by which the Services are required to be provided as set out in the Project Plan (if any);
"Service Credits"	the service credits payable by the Service Provider by way of a reduction in the Charges for failures to achieve the Service Levels as specified in the applicable Call-Off Contract
"Service Levels"	the service levels for the performance of the Products and Services specified in the Service Management Requirements and Technical Requirements Specification;
"Service Management Requirements"	the service management requirements for the provision of the Services as detailed in Schedule 5;

"Service Provider Equipment"	the equipment and materials of whatsoever nature used by the Service Provider in providing the Services which do not themselves form part of the Services and in which title is not intended to pass to TfL under any Call-Off Contract;
"Service Provider's Manager"	the person who is identified as the Service Provider's Manager in the Call-Off Contract for the relevant Services;
"Service Provider's Personnel"	all such employees, officers, suppliers, sub-contractors and agents of the Service Provider as are engaged in the performance of any of the Services and including the Key Personnel;
"Services"	(a) all or any part of the services to be provided to, or activities to be undertaken and completed for, TfL by the Service Provider as detailed in Schedule 3 and the Technical Requirements Specification and which shall be included under a Call-Off contract including any variations to such services and/or activities pursuant to Clause 32; and (b) any services, functions or responsibilities which may be reasonably regarded as incidental to the foregoing services or activities and which may be reasonably inferred from the Call-Off Contract;
"Special Conditions"	the terms and conditions detailed in Schedule 2 which are applicable to the performance of the Services;
"Technical Requirements Specification"	the technical requirements specification of the Services and other requirements set out in Schedule 3 and as may be additionally specified in any Call-Off Contract;
"Term"	the period during which this Agreement continues in force as set out in Schedule 1;
"Termination Charges"	the charges detailed in any relevant Call-Off Contract for termination of this Agreement and any other specific circumstances as detailed:

"TfL"	Transport for London, a statutory corporation established under the Greater London Authority Act 1999;
"TfL Group"	TfL and all its subsidiaries (as defined in section 736 of the Companies Act 1985) from time to time together with Cross London Rail Links Limited (company number 04212657) utilising this Agreement and reference to any "member of the TfL Group" shall refer to TfL or any such subsidiary;
"TfL Premises"	any land or premises (including temporary buildings) owned or occupied by or on behalf of any member of the TfL Group (including for the avoidance of doubt TfL);
"VAT"	means value added tax as provided for in the Value Added Tax Act 1994 and any tax replacing the same or of a similar nature; and
"Year"	a period of 12 months commencing on the Agreement Commencement Date and each period of 12 months commencing on the relevant anniversary thereafter.

1.2 a reference to the singular includes the plural and vice versa, and a reference to any gender includes all genders;

1.3 a reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended or re-enacted by any subsequent statute, enactment, order, regulation or instrument and shall include all statutory instruments or orders made pursuant to it whether replaced before or after the date of this Agreement;

1.4 a reference to any document other than as specified in Clause 1.3 and save as expressed otherwise shall be construed as a reference to the document as at the date of execution of this Agreement;

1.5 headings are included in the Agreement for ease of reference only and do not affect the interpretation or construction of the Agreement;

1.6 references to Clauses and Schedules are, unless otherwise provided, references to clauses of, and schedules to, the Agreement and any reference to a paragraph in any Schedule shall, in the absence of provision to the contrary, relate to the paragraph in that Schedule;

1.7 in the event, and only to the extent, of any conflict between the Clauses and the Schedules, the Clauses prevail, except where:

1.7.1 the conflicting part of the Schedule is explicitly expressed to take precedence; or

1.7.2 the conflict is with a provision in Schedule 2 (Special Conditions of Agreement), in which case the provisions in Schedule 2 shall prevail;

1.8 except as otherwise expressly provided in any Call-Off Contract, and subject to Clause 1.7, if there is any inconsistency between any of these Clauses, the Schedules, any Call-Off Contract or any other document referred to in or incorporated into this Agreement or any Call-Off Contract, the order of priority for the purposes of construction is:

1.8.1 each Call-Off Contract;

1.8.2 these Clauses;

1.8.3 the Schedules;

1.8.4 any other document referred to in or incorporated by reference into this Agreement or any Call-Off Contract;

1.9 the Schedules form part of the Agreement and subject to clause 1.8 will have the same force and effect as if expressly set out in the body of the Agreement;

1.10 the expression “person” means any individual, firm, body corporate, unincorporated association, partnership, government, state or agency of a state or joint venture; and

1.11 the words “including”, “includes” and “included” will be construed without limitation unless inconsistent with the context.

2. FRAMEWORK AGREEMENT

2.1 The purpose of this Agreement is to:

2.1.1 detail the Products and Services which TfL may require the Service Provider to supply from time to time in accordance with the terms of this Agreement;

2.1.2 provide a mechanism whereby the Parties may enter into Call-Off Contracts for the provision of the Products and Services;

2.1.3 provide the framework to administer each Call-Off Contract; and

2.1.4 set out the obligations of the Parties.

2.2 The Products and Services that may be requested by TfL and provided by the Service Provider are described in Schedule 3 and as more particularly described in the Technical Requirements Specification and/or each Call-Off Contract. TfL's requirements may vary and this Agreement shall not place TfL under any obligation to procure the Products or Services from the Service Provider at a particular time or at all. This Agreement is not an exclusive arrangement and nothing in this Agreement shall operate to prevent TfL from engaging any other organisations or persons to provide products or services similar to or the same as the Products or Services.

2.3 Clause 3 sets out the procedure by which the Parties may enter into a Call-Off Contract. Each Call-Off Contract shall be a binding agreement on the Parties and except as otherwise provided in each Call-Off Contract shall incorporate the terms and conditions of this Agreement.

2.4 The Service Provider shall commence provision of the relevant Products and Services in accordance with the Call-Off Contract. The Service Provider must not supply any Products or commence any Services and TfL and the GLA Bodies shall not seek to procure the same without an agreed Call-Off Contract.

3. CALL-OFF PROCEDURE

3.1 At any time during the duration of this Agreement, TfL may identify Products or Services which at its sole discretion it wishes to procure under the terms of this Agreement.

3.2 In such event TfL will issue to the Service Provider a Delivery Request Form substantially in the form set out in Schedule 7, specifying the Products and/or Services to be provided, in which event the Service Provider shall either promptly confirm acknowledgement and receipt of such Delivery Request Form or inform TfL of any reasons why the Products/and or Services requested cannot be delivered and what the Service Provider proposes as an alternative in either case via e-mail or as otherwise agreed by TfL within 2 Business Days of receiving the Delivery Request Form whereupon such acknowledgement shall constitute confirmation that the Service Provider shall provide the Products and Services as stated in the Delivery Request Form and the Delivery Request Form together with the acknowledgement will form a binding Call-Off Contract between the Parties.

3.3 Each Call-Off Contract shall be a binding agreement on the Parties and shall incorporate the terms and conditions of this Agreement and such documentation shall together form a separate agreement between the parties.

3.4 Unless otherwise expressly agreed in writing with TfL, the Service Provider shall not be entitled to charge under this Agreement for any work involved in any receipt and/or confirmation of any Delivery Request Form, and/or any response to any Delivery Request Form as contemplated in this clause 3.

3.5 Where reasonably requested to do so by any GLA Body, the Service Provider shall contract with such member of the GLA Body on the terms of this Agreement as may be amended by agreement between the Service Provider and the relevant GLA Body. For the avoidance of doubt, the GLA Bodies cannot affect or amend this Agreement and the Service Provider acknowledges that each Call-Off Contract shall be specifically between the Service Provider and the GLA Body and as such neither TfL or the TfL Group shall in any way be liable for the GLA Bodies' obligations arising out of such Call-Off Contract.

4. TERM OF AGREEMENT AND CALL-OFF CONTRACTS

4.1 This Agreement (but not a Call-Off Contract) commences on the Agreement Commencement Date and continues in force for the Term unless terminated earlier, either in whole or in part, in accordance with this Agreement.

4.2 Each Call-Off Term shall be set out in the relevant Call-Off Contract. The Parties acknowledge and agree that certain Products and/or Services have fixed terms or durations of use and various examples of these are listed in the table in Schedule 3. As such the Parties agree that whenever such Products and/or Services are purchased by TfL or any GLA Body from the Service Provider the Call-Off Term shall be commensurate with the fixed term or duration in the table unless specified otherwise in the Call-Off Contract. Unless stated otherwise in a Call-Off Contract, the Call-Off Term and the Services provided pursuant to a Call-Off Contract may extend beyond the termination or expiry of this Agreement, in which case the provisions of this Agreement shall survive such expiry or termination to the extent that such provisions are relevant to any such Call-Off Contract.

4.3 A Call-Off Contract may expire or be terminated in accordance with its terms or Clause 28 but such expiry or termination shall not, in and of itself, give rise to an expiry or termination of any other Call-Off Contract or this Agreement.

5. THE SUPPLY OF THE PRODUCTS / SERVICES

5.1 The Service Provider:

5.1.1 shall provide the Products and Services specified in a Call-Off Contract to TfL in accordance with this Agreement including for the avoidance of doubt the Special Conditions and the terms of the relevant Call-Off Contract.

5.1.2 acknowledges that it has sufficient information about TfL and the Technical Requirements Specification and that it has made all appropriate and necessary enquiries to enable it to supply the Products and perform the Services in accordance with this Agreement and the relevant Call-Off Contract;

5.1.3 shall comply with all lawful and reasonable directions of TfL relating to its supply of the Products and performance of the Services under any Call-Off Contract.

5.2 Notwithstanding anything to the contrary in this Agreement, TfL's discretion in carrying out its statutory duties shall not be fettered or otherwise constrained or affected by any provision of this Agreement or relevant Call-Off Contract;

5.3 The Service Provider shall provide the Services under each Call-Off Contract:

5.3.1 with the high degree of skill, care and diligence normally exercised by highly skilled and experienced wireless telecommunications service providers providing services of a similar scope, type and complexity to the Services and with sufficient resources including project management resources;

5.3.2 in conformance in all respects with the Technical Requirements Specification; and

5.3.3 in a safe manner and free from any unreasonable or avoidable risk to any person's health and well-being and in an economic and efficient manner.

5.4 The Service Provider shall deliver the Products to the Delivery Address on the Delivery Date or as agreed and risk and title in the Products shall pass to TfL upon delivery to the Delivery Address.

5.5 If the Service Provider at any time has reason to believe that it will be unable to deliver any Products to the Delivery Address on the Delivery Date, the Service Provider shall immediately notify TfL of the cause, the expected period of delay and the steps proposed by the Service Provider to minimise delay.

5.6 In the event that the Service Provider fails to deliver any Products to the Delivery Address on the Delivery Date:

5.6.1 Tfl shall be entitled to require the Service Provider, at its own expense, to arrange all such additional resources as may be necessary to ensure delivery of such Products to the Delivery Address as soon as is reasonably practicable thereafter; and

5.6.2 if the Service Provider fails to deliver the relevant Products to the Delivery Address within 2 Business Days of the Delivery Date ; then TfL shall be entitled to cancel the relevant Delivery Request Form (in whole or in part) by giving immediate written notice to the Service Provider and engage a third party to provide the Products and the Service Provider shall be liable in respect of all additional expenditure incurred by TfL in having such Products supplied by a third party.

5.6.3 The Service Provider shall not be liable for any failure to deliver in this Clause 5.6 to the extent that such failure is attributable to an act or omission of TfL or any member of the TfL Group.

5.7 Without prejudice to Clause 5.6 the Service Provider shall deliver the Products in accordance with the Service Levels. In the event of failures to perform in accordance with the Service Levels the Service Provider will credit TfL with the corresponding Service Credits as specified in Clause 6.6.

5.8 TfL shall be entitled to reject any Products delivered that are not in accordance with the relevant Delivery Request Form, the Technical Requirements Specification or the Special Conditions, and notwithstanding Clause 8 TfL shall not be deemed to have accepted any Products until it has had a reasonable time to inspect them following delivery.

5.9 Subject to Clause 3.2 whereby in the event that the Service Provider informs TfL of any reason why the Products and/or Services in a Delivery Request Form cannot be delivered as requested by TfL and TfL accepts any part deliveries of Products, TfL may reject the whole of the Products in a Delivery Request Form if an excess or shortfall in the quantity requested in the Delivery Request occurs notwithstanding the fact that the excess or shortfall may be slight.

5.10 The Service Provider shall provide TfL with any instructions or other information reasonably required to enable TfL to accept delivery of the Products.

6. CHARGES

6.1 The Charges for the Products and Services are set out in Schedule 6 and shall be applicable to each Call-Off Contract for the Products and Services unless agreed otherwise in writing by the Parties. The Service Provider shall invoice TfL in accordance with the procedures set out in Clause 7 and in consideration of, and subject to the due performance of the Services by the Service Provider, TfL shall pay the Service Provider the Charges in accordance with those procedures and any other terms and conditions of the relevant Call-Off Contract.

6.2 The Service Provider is not entitled to reimbursement for expenses unless such expenses are specified in a Call-Off Contract or have been incurred with the prior written consent of TfL, in which case the Service Provider shall supply appropriate evidence of expenditure in a form acceptable to TfL.

6.3 The Charges shall be benchmarked upon each anniversary of the Agreement Commencement Date in accordance with the provisions of Schedule 10.

6.4 All Charges exclude any VAT which may be chargeable, which will be payable in addition to the sum in question at the rate and in the manner for the time being prescribed by law on delivery of a valid VAT invoice.

6.5 If any Bespoke Products/Services (other than the Products and Services set out in Schedule 3) are agreed by the Parties to be supplied to TfL, TfL may, prior to agreeing the Charges request that the Service Provider demonstrates the price offering of the proposed Charges of the Bespoke Products/Services by allowing TfL to have visibility and access to the base book price and the final costs. In such instances the Parties will agree on a percentage addition to the book price in agreeing the Charges of the relevant Bespoke Products/Services.

6.6 **Service Credits**

If the Services are not supplied in accordance with the Service Levels the Service Provider will credit TfL with the corresponding Service Credits calculated in accordance with Schedule 5 or any relevant Call Off Contract (which will take effect as an adjustment to the Charges) within ten (10) days of the end of the relevant month. Subject to clause 6.6.2, the Service Credits due will be recovered by TfL as a credit against the next invoice for the Services, or if no such invoice is expected to become due within 30 days of the end of the relevant month, the Service Provider will pay TfL a sum equal to such Service Credit, within thirty (30) days of the date of the relevant credit note.

6.6.1 The right of TfL to any Service Credits will be without prejudice to any other rights which TfL may have under this Agreement or otherwise, including in particular the right to sue for damages, or other relief and /or terminate the affected Service or this entire Agreement or the relevant Call- Off Contract to which the services relate. . The fact that the Service Credit provisions anticipate or provide for a particular eventuality shall not be interpreted as implying that the relevant eventuality should not be considered a material breach of contract. Any Service Credit allowed in respect of a breach shall be treated as part payment of any damages awarded as a result of such breach and nothing in this Agreement will enable TfL to recover more than once in relation to the same loss.

6.6.2 If the Service Provider and TfL do not agree on the amount of any Service Credits to be offset against any Charges, the provisions of clause 27 (Dispute Resolution) will apply and pending such determination the disputed Service Credits will not be deducted from the relevant Charges. Any sums due to TfL or the Service Provider following resolution of the dispute on the Service Credits will be deducted from or added to (as the case may be) the instalment of the Charges due next following such resolution and, if no such Charges are due, as a debt due within 90 days of the resolution of the dispute.

7. PAYMENT PROCEDURES AND APPROVALS

7.1 The Service Provider shall invoice TfL in respect of the Charges:

7.1.1 for Airtime, (as defined in Schedule 2, Clause A6) monthly in arrears during the Call-Off Contract Term; or

7.1.2 at such dates or at the end of such other periods as may be specified in Schedule 6 and/or the relevant Call-Off Contract; or

7.1.3 if specified in a Call-Off Contract, on completion of each Milestone. It is a condition precedent of the submission of an invoice on completion of a Milestone that all preceding Milestones specified in the relevant Call-Off Contract have been completed

7.2 The Service Provider shall submit invoices to the address set out in each Call-Off Contract, each such invoice shall contain all information required by TfL including the Agreement Number, relevant Call-Off Contract Number, SAP order number, TfL Account Details, the Service Provider's name and address, a separate calculation of VAT and a brief description of the Services provided. Invoices shall be clear, concise, accurate, and adequately descriptive to avoid delays in processing subsequent payment.

7.3 In the event of a variation to the Products or Services in accordance with this Agreement or the relevant Call-Off Contract that involves the payment of additional charges to the Service Provider, the Service Provider shall identify these separately on the relevant invoice.

7.4 If TfL considers that the Charges claimed by the Service Provider in any invoice have under the relevant Call-Off Contract:

7.4.1 been correctly calculated and that such invoice is otherwise correct, the invoice shall be approved and payment shall be made by bank transfer (Bank Automated Clearance System (BACS)) or such other method as TfL may choose from time to time within 30 days of receipt of such invoice or such other time period as may be specified in the relevant Call-Off Contract;

7.4.2 not been calculated correctly and/or if the invoice contains any other error or inadequacy, TfL shall notify the Service Provider and the Parties shall work together to resolve the error or inadequacy. Upon resolution, the Service Provider shall submit a revised invoice to TfL.

7.5 No payment made by TfL (including any final payment) or act or omission or approval by TfL or contract Manager or Call-Off Co-ordinator (whether related to payment or otherwise) shall:

7.5.1 indicate or be taken to indicate TfL's acceptance or approval of the Products or Services or any part of them or any act or omission of the Service Provider, or otherwise prejudice any rights, powers or

remedies which TfL may have against the Service Provider, or absolve the Service Provider from any obligation or liability imposed on the Service Provider under this Agreement or a Call-Off Contract; or

7.5.2 prevent TfL from recovering any amount overpaid or wrongfully paid including payments made to the Service Provider by mistake of law or fact. Without prejudice to Clause 19, TfL shall be entitled to withhold such amount from any sums due or which may become due to the Service Provider or TfL may recover such amount as a debt under this Agreement or a Call-Off Contract.

8. WARRANTIES AND OBLIGATIONS

8.1 Without prejudice to any other warranties expressed elsewhere in this Agreement or implied by law, the Service Provider warrants, represents and undertakes that:

8.1.1 the Service Provider:

8.1.1.1 has full capacity and authority and all necessary licences, permits, permissions, powers and consents (including, where its procedures so require, the consent of its holding company as defined in section 736 of the Companies Act 1985) to enter into and to perform the Agreement and any relevant Call-Off Contract; and

8.1.1.2 acknowledges that TfL is reliant upon the Service Provider's expertise and knowledge in the provision of the Services; and

8.1.1.3 is entering into this Agreement and any relevant Call-Off Contract as principal and not as agent for any person and that it will act as an independent contractor in carrying out its obligations under this Contract;

8.1.2 this Agreement and all Call-Off Contracts are executed by a duly authorised representative of the Service Provider;

8.1.3 the Service Provider shall provide the Services:

8.1.3.1 in accordance with the relevant Call-Off Contract, the Special Conditions and the terms of this Agreement and with all due skill, care and diligence as may be expected of appropriately qualified and experienced persons (of a professional level if appropriate) with appropriate skill and experience in providing services of a similar scope, type, nature and complexity to the Services;

8.1.3.2 in a safe manner and free from any unreasonable or avoidable risk to any person's health and well-being and in an economic and efficient manner;

8.1.4 all Products and any other materials, equipment and goods under the relevant Call-Off Contract or supplied by the Service Provider will conform in all material respects to the manufacturer's warranties and specification which will be transferred to TfL and will be for at least a period of 12 months (but in the case of software 90 days) from the date on which each item is supplied to TfL or any greater period provided by the manufacturer (the "Warranty Period") ; and

8.1.5 the Products shall be Euro Compliant, unless the Service Provider informs TfL in writing that the Products are not Euro Compliant and in the event any Products are not Euro Compliant the Service Provider shall, if required by TfL, use all reasonable endeavours to ensure that the said Products become Euro Compliant as soon as reasonably possible and the Products shall not have their functionality or performance affected, be made inoperable or be more difficult to use by reason of any date related input or processing in or on any part of the Products;

8.1.6 the Products shall not cause any damage, loss or erosion to or interfere adversely or in any way with the compilation, content or structure of any data, database, software or other electronic or magnetic media, hardware or computer system used by, for or on behalf of TfL, on which it is used or with which it interfaces or comes into contact provided that TfL has complied with any instructions in the use of the Products provided by the Service Provider;

8.1.7 the Products shall comply with all statutory requirements and regulations relating to their sale and use;

8.1.8 the Service Provider shall provide TfL with adequate instructions to enable TfL to make full use of the Products;

8.1.9 TfL shall acquire the Products free from all encumbrances;

8.1.10 the Service Provider shall provide the Products in a safe manner and free from any unreasonable or avoidable risk to any person's health and well-being.

8.1.11 the use and/or possession of the Products by TfL and all documents, drawings, computer software and any other work prepared or developed by the Service Provider or supplied to TfL under the relevant Call-Off Contract shall not infringe any Intellectual Property Rights or any other legal or equitable right of any person.

8.2 Each warranty and obligation in this Clause 8 shall be construed as a separate warranty or obligation (as the case may be) and shall not be limited

or restricted by reference to, or reference from, the terms of any other such warranty or obligation or any other term of this Agreement.

8.3 With respect to any Products supplied under this Agreement that are not in accordance with any of the warranties specified in Clause 8.1, TfL, without prejudice to any of its other rights or remedies, may require the Service Provider immediately to:

8.3.1 repair or replace such Products with the same or equivalent Products of equal or better quality, which during the 'Dead on Arrival' period of at least 28 days from delivery of the Products to TfL shall be a new Product and thereafter may be new or refurbished Products, at the Service Provider's risk and expense; and

8.3.2 If the Service Provider is unable to repair or replace the Products in accordance with this Clause 8.3.1, then the Service Provider will refund to TfL the price paid by TfL in respect of such Products.

8.4 Products repaired or replaced in accordance with Clause 8.3.1 will be provided with a Warranty Period which shall last for the greater of: a) 3 months from the date on which the replacement Products are despatched to TfL or any greater Warranty Period given by the manufacturer; or b) the outstanding period of the original Warranty Period.

8.5 If the Service Provider refuses or fails promptly to repair or replace any Products when so requested to do so by TfL pursuant to Clause 8.3, TfL, without prejudice to any of its other rights and remedies, shall be entitled by itself, or through any agent or subcontractor, or otherwise, to repair or replace such Products.

8.6 For the purposes of construing the warranties in Clause 8.1, references to the Products include any part of the Products. Each warranty shall be construed as a separate warranty and shall not be limited or restricted by reference to, or reference from, the terms of any other warranty or any other term of this Agreement.

9. CONTRACTUAL MANAGEMENT

9.1 TfL authorises the Procurement Manager to act as TfL's representative for all purposes of this Agreement and the Service Provider shall deal with the Procurement Manager (or his or her nominated representative) in respect of all matters arising under this Agreement, unless notified otherwise. TfL will appoint a Call-Off Co-ordinator in respect of each Call-Off Contract in relation to matters arising under a Call-Off Contract, unless otherwise notified by TfL.

9.2 The Service Provider Manager shall act as the Service Provider's representative for all purposes of this Agreement. In respect of each Call-Off Contract, the Service Provider shall provide the Key Personnel. The Service Provider Manager and the Key Personnel and shall procure that they:

9.2.1 diligently supervise the performance of the Services;

9.2.2 attend all contract meetings with TfL (the location, frequency and time of which shall be by agreed in advance between the Service Provider Manager and the Procurement Manager or the relevant Call-Off Co-ordinator from time to time); and

9.2.3 be available to TfL to resolve any issues arising in connection with this Agreement or Call-Off Contract at such time periods as are specified in the relevant Call-Off Contract.

9.3 Any changes to the Service Provider Manager or Key Personnel will be subject to the prior written consent of TfL which shall not be unreasonably withheld and the Service Provider agrees that any proposed replacement will have the required experience and qualifications to perform the role satisfactorily and professionally. 9.4 The Service Provider shall not be liable for any loss which arises to the extent that such loss arises as a result of a failure to act of or omission by or approval from either TfL, the Procurement Manager, or any Call-Off Co-ordinator in performing any of their respective duties under or in connection with this Agreement or relevant Call-Off Contract.

10. SERVICE PROVIDER'S PERSONNEL

10.1 Nothing in this Agreement or any Call-Off Contract will render the Service Provider's Personnel, an employee, agent or partner of TfL or of any member of the TfL Group by virtue of the provision of the Services by the Service Provider under this Agreement or Call-Off Contract and the Service Provider shall be responsible for making appropriate deductions for tax and national insurance contributions from the remuneration paid to the Service Provider's Personnel.

10.2 The Service Provider shall provide the Service Provider's Personnel as necessary for the proper and timely performance and management of the Services in accordance with the relevant Call-Off Contract but for the avoidance of doubt, time shall not be of the essence.

10.3 Without prejudice to any of TfL's other rights, powers or remedies, TfL may (without liability to the Service Provider) deny access to such Service Provider's Personnel to any TfL Premises if such Service Provider's Personnel in TfL's view have not been properly trained in any way required by a relevant Call-Off Contract and/or are otherwise incompetent, negligent, and/or guilty of misconduct and/or who could be a danger to any person and TfL shall notify the Service Provider of such denial in writing; the Service Provider shall immediately remove such Service Provider's Personnel from performing the Services and provide a suitable replacement (with the Call-Off Co-ordinator's prior consent in the case of Key Personnel).

10.4 The Service Provider shall indemnify, keep indemnified and hold harmless TfL from and against all liabilities, costs, expenses, injuries, direct or indirect or

consequential loss, damages, claims, demands, proceedings and legal costs (on a full indemnity basis) which TfL or the TfL Group incur or suffer whenever arising as brought by the Service Provider's Personnel or any person who may allege to be the same.

11. SUB-CONTRACTING AND CHANGE OF OWNERSHIP

11.1 The Service Provider shall not assign or sub-contract all or any part of the Services without the prior written consent of TfL identifying the relevant sub-contractor which may be refused or granted subject to such conditions as TfL sees fit. Subject to the Service Provider complying with Schedule 2, Clause A9.1 TfL consents to the sub-contractors which the Service Provider appoints for use as at the Agreement Commencement Date.

11.2 Where the Service Provider sub-contracts all or any part of the Services to any person, the Service Provider shall:

11.2.1 ensure that such person is obliged to comply with all of the obligations and duties of the Service Provider under the relevant Call-Off Contract insofar as they relate to the Services or part of them (as the case may be) which that sub-contractor is required to provide;

11.2.2 be responsible for payments to that person; and

11.2.3 remain solely responsible and liable to TfL for any breach of the relevant Call-Off Contract or any performance, non-performance, part-performance or delay in performance of any of the Services by any sub-contractor to the same extent as if such breach, performance, non-performance, part-performance or delay in performance had been carried out by the Service Provider.

11.3 The Service Provider shall:

11.3.1 inform TfL by written notice of any change in the ownership of the Service Provider where such change relates to 50% or more of the issued share capital of the Service Provider; and

11.3.2 give notice to TfL in the event that there is any change in the ownership of the Holding Company where such change relates to 50% or more of the issued share capital of the Holding Company, such notice to be given within 10 Business Days of the date on which such change takes effect.

12. CONFLICT OF INTEREST

12.1 The Service Provider warrants that it does not and will not have any interest in any matter where there is or is reasonably likely to be a conflict of interest with the Services or any member of the TfL Group, save to the extent fully disclosed to and approved by TfL.

12.2 The Service Provider shall check for any conflict of interest at regular intervals throughout the duration of this Agreement and in any event not less than once in every six months and shall notify TfL in writing immediately upon becoming aware of any actual or potential conflict of interest with the Services or any member of the TfL Group and shall work with TfL to do whatever is necessary (including the separation of staff working on, and data relating to, the Services from the matter in question) to manage such conflict to TfL's satisfaction, provided that, where TfL is not so satisfied, it may terminate this Agreement and all Call-Off Contracts, in existence, in accordance with Clause 28.1.4.

13. ACCESS TO PREMISES

13.1 Subject to Clause 10.3 any access to any TfL Premises made available to the Service Provider in connection with the proper performance of the Call-Off Contract shall be free of charge and shall be used by the Service Provider solely for the purpose of performing the Services during the Call-Off Contract Term, for the avoidance of doubt, that the Service Provider shall be responsible for its own costs or travel including any congestion charging. The Service Provider shall:

13.1.1 have the use of such TfL Premises as licensee and shall not have or purport to claim any sole or exclusive right to possession or to possession of any particular part of such TfL Premises;

13.1.2 vacate such TfL Premises upon the termination or expiry of the relevant Call-Off Contract or at such earlier date as TfL may determine;

13.1.3 not exercise or purport to exercise any rights in respect of any TfL Premises in excess of those granted under this Clause 13.1;

13.1.4 take all practicable steps to ensure that the Service Provider's Personnel carry any identity passes issued to them by TfL at all relevant times and comply with TfL's security procedures as may be notified by TfL from time to time; and

13.1.5 take all practicable steps to not damage the TfL Premises or any assets on the TfL Premises.

13.2 Nothing in this Clause 13 shall create or be deemed to create the relationship of landlord and tenant in respect of any TfL Premises between the Service Provider and any member of the TfL Group.

13.3 TfL shall be under no obligation to provide office or other accommodation or facilities or services (including telephony and IT services) to the Service Provider except as may be specified in any Call-Off Contract.

14. COMPLIANCE WITH POLICIES AND LAW

14.1 The Service Provider, at no additional cost to TfL:

14.1.1 undertakes to take all reasonable steps to procure that all the Service Provider's Personnel comply with all of TfL's policies and standards that are relevant to the performance of the Services, including the provisions set out in Schedule 9 and those relating to safety, security, business ethics, drugs and alcohol and any other on site regulations specified by TfL for personnel working at TfL Premises or accessing TfL's computer systems. TfL shall provide the Service Provider with copies of such policies and standards on request;

14.1.2 shall provide the Services in compliance with all requirements of all Acts of Parliament, statutory instruments, court orders, regulations, directives, European Community decisions (insofar as legally binding), bye-laws, treaties and other regulatory requirements relevant to the Service Provider's business and/or TfL's business, from time to time in force which are or may become applicable to the Services. The Service Provider shall promptly notify TfL if the Service Provider is required to make any change to the Services for the purposes of complying with its obligations under this Clause 14.1.2;

14.1.3 without limiting the generality of Clause 14.1.2, shall comply with all relevant enactments in force from time to time relating to discrimination in employment and the promotion of equal opportunities;

14.1.4 acknowledges that TfL is under a duty under section 71 of the Race Relations Act 1976 and under section 49A of the Disability Discrimination Act 1995 to have due regard to the need to eliminate unlawful discrimination on the grounds of race or disability (as the case may be) and to promote equality of opportunity between persons of different racial groups and between disabled people and other people (as the case may be). In providing the Services, the Service Provider shall assist and co-operate with TfL where possible in satisfying this duty;

14.1.5 acknowledges that TfL is under a duty by virtue of a direction under section 155 of the Greater London Authority Act 1999 in respect of section 404(2) of that Act to have due regard to the need to:

14.1.5.1 promote equality of opportunity for all persons irrespective of their race, sex, disability, age, sexual orientation or religion;

14.1.5.2 eliminate unlawful discrimination; and

14.1.5.3 promote good relations between persons of different racial groups, religious beliefs and sexual orientation,

and in providing the Services, the Service Provider shall assist and co-operate with TfL where possible to enable TfL to satisfy its duty;

14.1.6 without prejudice to any other provision of this Clause 14.1 or the Schedules, shall comply with any provisions set out in the Schedules that relate to traffic management and shall comply with the reasonable instructions of TfL's Traffic Manager as may be made available to the Service Provider from time to time. For the purposes of this Clause 12.1.6, "Traffic Manager" means TfL's traffic manager appointed in accordance with section 17 of the Traffic Management Act 2004; and

14.1.7 shall promptly notify the Service Provider's Personnel and TfL of any health and safety hazards that exist or may arise in connection with the performance of the Services.

In all cases, the costs of compliance with this Clause 14.1 shall be borne by the Service Provider.

14.2 Without prejudice to Clause 14.1, whilst on TfL's premises, the Service Provider shall comply with TfL's workplace harassment policy as updated from time to time (copies of which are available on request from TfL) and with TfL's Code of Conduct (which is available on TfL's website, www.tfl.gov.uk).

14.3 In providing the Services, the Service Provider shall (taking into account best available techniques not entailing excessive cost and the best practicable means of preventing, or counteracting the effects of any noise or vibration) have appropriate regard (insofar as the Service Provider's activities may impact on the environment) to the need to:

14.3.1 preserve and protect the environment and to the need to avoid, remedy and mitigate any adverse effects on the environment;

14.3.2 enhance the environment and have regard to the desirability of achieving sustainable development;

14.3.3 conserve and safeguard flora, fauna and geological or physiological features of special interest; and

14.3.4 sustain the potential of natural and physical resources and the need to safeguard the life-supporting capacity of air, water, soil and ecosystems.

15. CORRUPT GIFTS AND PAYMENT OF COMMISSION

The Service Provider shall not, and shall ensure that its employees, agents and sub-contractors do not, pay any commission, fees or grant any rebates to any employee, officer or agent of TfL or any member of the TfL Group nor favour any employee, officer or agent of TfL or any member of the TfL Group with gifts or entertainment of significant cost or value nor enter into any business arrangement with employees, officers or agents of TfL or any member of the TfL Group other than as a representative of TfL, without TfL's prior written approval.

16. SERVICE PROVIDER EQUIPMENT

16.1 Risk in:

16.1.1 all Service Provider Equipment shall be with the Service Provider at all times; and

16.1.2 all other equipment and materials forming part of the Services (title to which will pass to TfL) (**"Materials"**) shall be with the Service Provider at all times until completion of the Services in accordance with the relevant Call-Off Contract.

regardless of whether or not the Service Provider's Equipment and Materials are located at TfL Premises:

16.2 The Service Provider shall ensure that all Service Provider's Equipment and all Materials meet all minimum safety standards required from time to time by law.

17. QUALITY AND BEST VALUE

The Service Provider acknowledges that TfL is a best value authority for the purposes of the Local Government Act 1999 and as such TfL is required to make arrangements to secure continuous improvement in the way it exercises its functions, having regard to a combination of economy, efficiency and effectiveness, as such, the Service Provider shall, where reasonably requested by TfL, participate in any relevant best value review.

18. RECORDS, AUDIT AND INSPECTION

18.1 The Service Provider shall, and shall procure that its sub-contractors shall:

18.1.1 maintain complete and correct set of records pertaining to all activities relating to the performance of the Services and the Service Provider's obligations under this Agreement and the relevant Call-Off Contract and all transactions entered into by the Service Provider for the purposes of this Agreement (including time-sheets for the Service Provider's Personnel where such records are material to the calculation of the Charges) (**"Records"**);

18.1.2 retain all Records during the Term and Call-Off Term and for a period of not less than 6 years (or such longer period as may be required by law) following termination or expiry of this Agreement or relevant Call-Off Contract (**"Retention Period"**).

18.2 TfL and any person nominated by TfL has the right to audit any and all Records at any time during the Retention Period on giving to the Service Provider reasonable notice (whether in writing or verbally) and at any reasonable time during the ordinary hours of the Service Provider's business

on a Business Day to inspect any aspect of the Service Provider's performance of the Services and the Service Provider shall give all reasonable assistance to TfL or its nominee in conducting such inspection, including making available documents and staff for interview.

18.3 The Service Provider shall, on a quarterly basis in arrears, the first quarter commencing on the Agreement Commencement Date, submit a report to TfL detailing:-

18.3.1 the % amount of recycled material within the Products supplied to TfL where this information is made available to the Service Provider;

18.3.2 the quantity of Products purchased; and

18.3.3 the quantity of the Products that are recycled and/or re-used.

19. SET-OFF

Each Party will be entitled but not obliged at any time or times to set off any liability of that Party to the other Party against any liability of the other Party to the first mentioned Party.

20. INDEMNITY

20.1 Subject to Clause 20.2, 20.3 and 20.4 the Service Provider is responsible for and shall indemnify, keep indemnified and hold harmless TfL and the other members of the TfL Group (including their respective employees, sub-contractors and agents) (**"the Indemnified Party"**) against a maximum of £5,000,000 (five million pounds sterling) of Direct Losses which the Indemnified Party incurs or suffers in aggregate in each year of this Agreement (where "Year" means the consecutive period of 12 months commencing on the Agreement Commencement Date and each anniversary thereof) as a consequence of any breach or any negligent performance of this Agreement or any relevant Call-Off Contract by the Service Provider (or any of its employees, agents or sub-contractors) (including in each case any non-performance or delay in performance of this Agreement) or of any breach of statutory duty, misrepresentation or misstatement by the Service Provider (or any of its employees or sub-contractors). For the avoidance of doubt, and subject to Clauses 20.3 and 20.4, the Service Provider shall not be liable for losses which are not Direct Losses.

20.2 The Service Provider is not responsible for and shall not indemnify TfL for any losses to the extent that such losses are caused by any breach or negligent performance of any of its obligations under this Agreement or Call-Off Contract by TfL and/or any other member of the TfL Group including by any of their respective employees or agents.

20.3 The maximum sum of liability in clause 20.1 shall not be applicable to Schedule 2, Clause A4 (Intellectual Property Infringement) Clause 24

(Protection of Personal Data) and Clause 25 (Confidentiality) which liability shall be unlimited.

20.4 Neither Party excludes or limits it's liability to the other Party for fraud or for death or personal injury caused by its negligence.

20.5 TfL's liability under this Agreement shall not exceed a maximum of £5,000,000 for all Direct Losses which the Service Provider incurs or suffers in aggregate in each Year of this Agreement (as defined in Clause 20.1 above) as a consequence of any breach or any negligent performance of this Agreement or any relevant Call-Off contract by TfL (or any of its employees, agents or sub-contractors) (including in each case any non-performance or delay in performance of this Agreement) or of any breach of statutory duty, misrepresentation or misstatement by TfL (or any of its employees or sub-contractors). For the avoidance of doubt, and subject to Clause 20.4, TfL shall not be liable for losses which are not Direct Losses.

21. INSURANCE

21.1 The Service Provider will at its sole cost maintain employer's liability and motor insurance cover as required by law and insurance cover in the sum of £5 million per claim (in terms approved by TfL) in respect of the following to cover the Services (**"the Insurances"**) and the additional insurance (if any) specified in Schedule 1:

21.1.1 public liability to cover injury and loss to third parties;

21.1.2 insurance to cover the loss or damage to any item related to the Services;

21.1.3 product liability; and

21.1.4 professional indemnity or, where professional indemnity insurance is not available, a "financial loss" extension to the product liability insurance referred to in Clause 21.1.3.

21.2 The insurance cover will be maintained with a reputable insurer with the prior approval of TfL(such approval not to be unreasonably withheld or delayed).

21.3 The Service Provider will produce evidence to TfL on reasonable request of the insurance policies set out in Clause 21.1 and payment of all premiums due on each policy.

21.4 The Service Provider warrants that nothing has or will be done or be omitted to be done which may result in any of the insurance policies set out in Clause 21.1 being or becoming void, voidable or unenforceable.

22. TFL'S DATA

22.1 The Service Provider acknowledges TfL's ownership of Intellectual Property Rights which may subsist in TfL's data. The Service Provider shall not delete or remove any copyright notices contained within or relating to TfL's data.

22.2 The Service Provider and TfL shall each take reasonable precautions (having regard to the nature of their other respective obligations under this Agreement) to preserve the integrity of TfL's data and to prevent any corruption or loss of TfL's data.

23. INTELLECTUAL PROPERTY RIGHTS

23.1 The Intellectual Property Rights in any Products and/or Services (other than any Bespoke Products/Services) shall vest in the Service Provider, or the owner if not the Service Provider, and the Service Provider grants to TfL a perpetual, royalty free and transferable licence to use any such Intellectual Property Rights for the purposes of the use of the Products and the Services.

23.2 The Intellectual Property Rights in any Bespoke Products/Services shall vest in TfL unless agreed otherwise by the Parties and the Service Provider shall take all steps required to vest or assign the Intellectual Property Rights in TfL.

23.3 The Service Provider shall indemnify TfL in accordance with clause A4 in Schedule 2 in respect of any infringement or alleged infringement of any Intellectual Property Rights.

23.4 The Service Provider shall provide TfL with copies of all materials relied upon or referred to in the creation of the Materials with a perpetual, irrevocable, royalty-free and transferable licence free of charge to use such materials in connection with the use of the Materials.

24. PROTECTION OF PERSONAL DATA

The Service Provider shall comply with all of its obligations under the Data Protection Act 1998 and, if Processing Personal Data (as such terms are defined in section 1(1) of that Act) on behalf of TfL, shall only carry out such Processing for the purposes of providing the Services in accordance with this Agreement and any relevant Call-Off Contract and shall act in accordance with the Special Conditions in respect of Data Protection.

25. CONFIDENTIALITY AND ANNOUNCEMENTS

25.1 Subject to Clause 26, each Party will keep confidential:

25.1.1 the terms of this Agreement and all Call-Off Contracts; and

25.1.2 any and all Confidential Information that it may acquire in relation to the other Party.

25.2 Neither Party will use the other Party's Confidential Information for any purpose other than to perform its obligations under this Agreement. Each Party will ensure that its officers and employees comply with the provisions of Clause 25.1.

25.3 The obligations on a Party set out in Clause 25.1 will not apply to any Confidential Information which:

25.3.1 either of the Parties can demonstrate is in the public domain (other than as a result of a breach of this Clause 25); or

25.3.2 a Party is required to disclose by order of a court of competent jurisdiction but then only to the extent of such required disclosure; or

25.3.3 the Service Provider is required to disclose pursuant to clause 28.1.

25.4 The provisions of this Clause 25 will survive any termination of this Agreement or Call-Off Contract for a period of 5 years from termination.

26. FREEDOM OF INFORMATION

26.1 For the purposes of this Clause 26:

26.1.1 **"FOI Legislation"** means the Freedom of Information Act 2000, all regulations made under it and the Environmental Information Regulations 2004 and any amendment or re-enactment of any of them; and any guidance issued by the Information Commissioner, the Department for Constitutional Affairs, or the Department for Environment Food and Rural Affairs (including in each case its successors or assigns) in relation to such legislation;

26.1.2 **"Information"** means information recorded in any form held by TfL or by the Service Provider on behalf of TfL; and

26.1.3 **"Information Request"** means a request for any Information under the FOI Legislation.

26.2 The Service Provider acknowledges that TfL:

26.2.1 is subject to the FOI Legislation and agrees to assist and co-operate with TfL to enable TfL to comply with its obligations under the FOI Legislation; and

26.2.2 may be obliged under the FOI Legislation to disclose Information without consulting or obtaining consent from the Service Provider.

26.3 Without prejudice to the generality of Clause 26.2, the Service Provider shall and shall use all reasonable endeavours to procure that its sub-contractors (if any) shall:

26.3.1 transfer to the Procurement Manager (or such other person as may be notified by TfL to the Service Provider) each Information Request relevant to this Agreement or a Call-Off Contract, the Services that it or they (as the case may be) receive as soon as practicable and in any event within 2 Business Days of receiving such Information Request; and

26.3.2 in relation to Information held by the Service Provider on behalf of TfL, provide TfL with details about and/or copies of all such Information that TfL requests and such details and/or copies shall be provided within 5 Business Days of a request from TfL (or such other period as TfL may reasonably specify), and in such forms as TfL may reasonably specify.

26.4 TfL shall be responsible for determining whether Information is exempt information under the FOI Legislation and for determining what Information will be disclosed in response to an Information Request in accordance with the FOI Legislation. The Service Provider shall not itself respond to any person making an Information Request, save to acknowledge receipt, unless expressly authorised to do so by TfL.

27. DISPUTE RESOLUTION

27.1 TfL and the Service Provider shall use all reasonable endeavours to negotiate in good faith and settle any dispute or difference that may arise out of or relate to this Agreement or any relevant Call-Off Contract (**"Dispute"**) before resorting to litigation.

27.2 If the Dispute is not settled through discussion between the Contract Manager and a representative of the Service Provider within a period of seven Business Days of the date on which the Dispute arose, the Parties may refer the Dispute in writing to a director or chief executive (or equivalent) (**"Senior Personnel"**) of each of the Parties for resolution.

27.3 If the Dispute is not resolved within 14 Business Days of referral to the Senior Personnel, either Party may propose by notice to the other Party (**"Notice"**) that a structured mediation or negotiation be entered into with the assistance of a mediator.

27.4 If both Parties are willing to submit to mediation and the Parties are unable to agree on a mediator, or if the agreed mediator is unable or unwilling to act within 28 Business Days of the service of the Notice, either Party may apply to the Centre for Effective Dispute Resolution (**"CEDR"**) in London to appoint a mediator. The costs of that mediator shall be divided equally between the Parties or as the Parties may otherwise agree in writing.

27.5 Where a dispute is referred to mediation under Clause 27.3, the Parties will attempt to settle such Dispute by mediation in accordance with the model mediation procedures published by CEDR or such other procedures as the mediator may recommend.

27.6 If the Parties reach agreement on the resolution of the Dispute, such agreement shall be recorded in writing and once signed by the Parties' authorised representatives, shall be final and binding on the Parties.

27.7 If either Party refuses at any time to participate in the mediation procedure and in any event if the Parties fail to reach agreement on the Dispute within 40 Business Days of the service of the Notice either Party may commence proceedings in accordance with Clause 41.

27.8 For the avoidance of doubt, the Service Provider shall continue to provide the Services in accordance with the Call-Off Contract and without delay or disruption while the Dispute is being resolved pursuant to this Clause 27.

27.9 Neither Party shall be prevented from, or delayed in, seeking any order for specific performance or for interim or final injunctive relief as a result of the provisions of this Clause 27 and Clause 27 shall not apply in respect of any circumstances where such remedies are sought.

28. BREACH AND TERMINATION OF AGREEMENT

28.1 Without prejudice to either Party's rights to terminate at common law, a Party (which may include a member of the TfL Group) ("**Terminating Party**") may terminate this Agreement and a Terminating Party or the Terminating Party's Group Member(s) in the case of TfL(as the case may be) may terminate any current Call-Off Contract immediately upon giving notice to the other Party if:

28.1.1 except as provided in and without prejudice to Clauses 28.1.3, the Terminating Party has committed any material or persistent breach of this Agreement (where TfL or the Service Provider is the Terminating Party) or Call-Off Contract (where TfL, a member of the TfL Group or the Service Provider is the Terminating Party) and in the case of such a breach that is capable of remedy fails to remedy that breach within 10 Business Days (or such other timeframe as specified in writing by the Terminating Party) from the date of written notice to the other Party giving details of the breach and requiring it to be remedied; or

28.1.2 in the arise of a material or persistent breach of this Agreement by TfL for non-payment of invoices the Service Provider shall provide TfL with written notice of non-payment of such invoices requiring the breach to be remedied and, unless such invoice(s) are subject to a bona-fide dispute between the Parties which shall be dealt with in accordance with clause 27, in the event TfL does not pay such invoice(s) within 30 days of written notice from the Service Provider the Service Provider shall be entitled to terminate this Agreement or any current Call-Off Contract which is subject to the breach.

28.1.3 the other Party is subject to an Insolvency Event; or

28.1.4 the Service Provider is in breach of Clause 11.3; or

28.1.5 TfL can establish that it has legitimate reasons in respect of any conflict of interest in accordance with Clause 12 which requires TfL to terminate this Agreement; or

28.1.5 the Service Provider commits any of the money laundering related offences listed in the Public Agreement Regulations 2006.

28.2 Without prejudice to any of TfL's and/or TfL Group Member(s) other rights, powers or remedies (whether under this Agreement or otherwise) if the Service Provider is in breach of any of its warranties and/or obligations under Clause 8 and/or any of its other obligations in respect of the Products and/or Services under this Agreement or Call-Off Contract, the Service Provider shall, if required to do so by TfL's and/or the TfL Group Member(s), within a timescale reasonably required by TfL remedy and/or re-perform the Services or part of them at its own expense to ensure compliance with such warranties and/or obligations. In the event that the Service Provider fails to remedy or and/or re-perform the Services in the required timescale TfL and/or the TfL Group Member(s) may procure the provision of any Services or any remedial action in respect of any Services from an alternative service provider and, where TfL and/or the TfL Group Member(s) so procures any Services or any remedial action, TfL and/or the TfL Group Member(s) shall be entitled to recover from the Service Provider all additional cost, loss and expense incurred by TfL and/or the TfL Group Member(s) and attributable to TfL and/or the TfL Group Member(s) procuring such Services or remedial action from such alternative service provider.

28.3 Neither Party shall be deemed to be in breach of the relevant Call-Off Contract, or otherwise liable to the other Party in any manner whatsoever, for any failure or delay in performing its obligations under the relevant Call-Off Contract to the extent that such failure or delay is due to a Force Majeure Event. If a Force Majeure Event has continued for more than 8 weeks from the date on which that Force Majeure Event first arose, then for as long as such Force Majeure Event continues and has that effect, the Party not affected by such Force Majeure Event (**"Unaffected Party"**) may terminate the Call-Off Contract immediately upon giving notice to the Party affected by the Force Majeure Event (**"Affected Party"**). If the Call-Off Contract is terminated in accordance with this Clause 28.3 then without prejudice to any rights and liabilities which accrued prior to termination the Affected Party shall not be liable to the Unaffected Party by reason of such termination.

28.4 Without prejudice to TfL's right to terminate this Agreement or TfL and/or the TfL Group Member(s) to terminate the relevant Call-Off Contract under Clause 28.1 or to terminate at common law, TfL may terminate this Agreement or TfL and/or the TfL Group Member(s) the relevant Call-Off Contract at any time without cause subject to giving the Service Provider written notice of the period specified in Schedule 1, provided that this Clause 28.4 may be disapplied by notice to that effect in Schedule 1.

28.5 To the extent that TfL has a right to terminate this Agreement or TfL and/or the TfL Group Member(s) the relevant Call-Off Contract under this Clause 28 then, as an alternative to termination, TfL may by giving notice to the Service Provider require the Service Provider to provide part only of the Services with effect from the date specified in TfL's notice (**"Change Date"**) whereupon the provision of the remainder of the Services will cease and the definition of "the Services" shall be construed accordingly. The Charges applicable with effect from the Change Date will be adjusted proportionately or as otherwise agreed between the Parties..

29. CONSEQUENCES OF TERMINATION OR EXPIRY

29.1 Notwithstanding the provisions of Clause 25, wherever TfL chooses to put out to tender for a replacement service provider some or all of the Services, the Service Provider shall disclose to tenderers such information concerning the Services as TfL may reasonably require for the purposes of such tender provided that nothing in this clause shall require the Service Provider to disclose any of the Service Provider's Confidential Information unless such Confidential Information is required to be disclosed by TfL by law and as a pre-condition to disclosure pursuant to this clause, the Service Provider may impose upon any recipient of such information such obligations of confidentiality as it may require.

29.2 The termination or expiry of this Agreement shall not prejudice or affect any right, power or remedy which has accrued or shall accrue to either Party prior to or after such termination or expiry.

29.3 Upon expiry or termination of this Agreement or relevant Call-Off Contract (howsoever caused):

29.3.1 the Service Provider shall, at no further cost to TfL:

29.3.1.1 on receipt of TfL's written instructions to do so (but not otherwise), arrange to remove all electronically held information by a mutually agreed date, including the purging of all disk-based information and the reformatting of all disks.

29.3.2 TfL shall (subject to Clauses 19, 29.1 and 29.4 and the provisions of any security for due performance supplied by the Service Provider) pay the Service Provider any Charges remaining due in relation to any Services properly performed in accordance with the relevant Call-Off Contract up to the date of termination or expiry calculated so far as is possible in accordance with the rules set out in the Call-Off Contract.

29.4 In the event that this Agreement is terminated by the Service Provider pursuant to Clauses 28.1.1, 28.1.2, 28.1.3 or is terminated by TfL pursuant to Clause 28.4 the Termination Charges as set out in Schedule 6 shall be payable by TfL to the Service Provider.

29.5 Notwithstanding the provisions of clause 20.1, on termination of this Agreement and any relevant Call-Off Contract under Clause 28.1 or a cessation of any Services under Clause 28.4 (but in the case of the latter only insofar as the right to cease any Services arises as a result of a right for TfL to terminate under Clause 28.1), TfL may enter into any agreement with any third party or parties as TfL thinks fit to provide any or all of the Services and the Service Provider shall be liable for all additional expenditure reasonably incurred by TfL in having such services carried out and all other costs and damages reasonably incurred by TfL in consequence of such termination. TfL may deduct such costs from the Charges or otherwise recover such costs from the Service Provider as a debt.

30. BUSINESS CONTINUITY

30.1 The Service Provider will ensure that at all times it has in place business continuity plans to allow it to comply with Schedule 11.

30.2 The Business Continuity Plan will be tested in accordance with the provisions of Schedule 11. It will be adjusted promptly by the Service Provider as necessary to take into account any change to the Services made in accordance with clause 33 or as otherwise agreed by the Parties.

30.3 Where the Service Provider can demonstrate that a Disaster was caused by Force Majeure the provisions of clause 28.3 will apply, but only to the extent that such Disaster prevents the Service Provider from satisfying its obligations and the requirement to pay Service Credits will cease to apply in respect of such element(s) until such time as the provision of the Services are resumed or ought to have been resumed, whichever is the earlier, in accordance with the Business Continuity Plan.

30.4 Where a Disaster arises from circumstances other than those set out in clause 28.3**,** the Service Provider's liability to pay Service Credits shall continue to accrue until such time as the Services are performed by the Service Provider in accordance with the provisions of this Agreement.

30.5 Following declaration of a Disaster, the Service Provider shall forthwith implement the Business Continuity Plan and shall continue to provide those Services which are not affected (or to the extent parts are not affected, those parts) by the Disaster in accordance with the provisions of this Agreement. In respect of those Services which are affected by the Disaster, the Service Provider shall provide those Services to at least the level set out in the Business Continuity Plan as applicable for the relevant Service.

31. SURVIVAL

The provisions of Clauses 1, 6, 7, 8, 11.2.2, 11.2.3, 13.1.1, 13.1.2, 13.1.5, 13.2, 16, 18-22 (inclusive), 23.2, 24-27 (inclusive), 29-33 (inclusive), 35-41 (inclusive) and any other Clauses or Schedules that are necessary to give

effect to those Clauses shall survive termination or expiry of this Agreement. In addition, any other provision of this Agreement which by its nature or implication is required to survive the termination or expiry of this Agreement or relevant Call-Off Contract shall do so.

32. RIGHTS OF THIRD PARTIES

32.1 Save that any member of the TfL Group has the right to enforce the terms of this Agreement or any relevant Call-Off Contract in accordance with the Contracts (Rights of Third Parties) Act 1999 ("Third Party Act"), subject to Clause 27 in the first instance of a dispute, the Parties do not intend that any of the terms of this Agreement or any relevant Call-Off Contract will be enforceable by virtue of the Third Party Act by any person not a party to it.

32.2 Notwithstanding Clause 32.1, the Parties are entitled to vary or rescind this Agreement or any relevant Call-Off Contract without the consent of any or all members of the TfL Group.

33. CONTRACT VARIATION

This Agreement or Call-Off Contract may only be varied or amended with the written agreement of both Parties. The details of any variations or amendments shall be set out in such form as TfL may dictate and which may be substantially in the form set out in Schedule 8 and shall not be binding upon the Parties unless completed in accordance with such form of variation.

34. NOVATION

34.1 TfL may novate or otherwise transfer this Agreement and TfL and/or the TfL Group Member(s) any relevant Call-Off Contracts (in whole or in part) to any third party capable at the time of novation or other transference, of fulfilling all TfL's obligations.

34.2 Within 10 Business Days of a written request from TfL and/or the TfL Group Member(s), the Service Provider shall execute such agreement as TfL and/or the TfL Group Member(s) may reasonably require to give effect to any such transfer all or part of its rights and obligations under this Agreement and any relevant Call-Off Contract to one or more persons nominated by TfL and/or the TfL Group Member(s). TfL shall reimburse any reasonable third-party costs incurred by the Service Provider in complying with this Clause 34.2.

34.3 Subject to Clause 11, this Agreement is personal to the Service Provider who shall not assign the benefit or delegate the burden of this Agreement (excluding permitted sub-contracting under Clause 11.1) or otherwise transfer any right or obligation under this Agreement without the prior written consent of TfL.

35. NON-WAIVER OF RIGHTS

No waiver of any of the provisions of this Agreement or any relevant Call-Off Contract is effective unless it is expressly stated to be a waiver and communicated to the other Party in writing in accordance with the provisions of Clause 37. The single or partial exercise of any right, power or remedy under this Agreement shall not in any circumstances preclude any other or further exercise of it or the exercise of any other such right, power or remedy.

36. ILLEGALITY AND SEVERABILITY

If any provision of this Agreement (in whole or in part) is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision shall be severed from this Agreement and the remaining provisions shall continue in full force and effect as if this Agreement had been executed without the invalid, illegal, or unenforceable provision. In the event that in a Party's reasonable opinion such a provision is so fundamental as to prevent the accomplishment of the purpose of this Agreement, TfL and the Service Provider shall immediately commence good faith negotiations to remedy such invalidity.

37. NOTICES

Subject to Clause 37.2, any notice, demand or communication in connection with this Agreement will be in writing and may be delivered by hand, post or facsimile addressed to the recipient at its registered office, the address stated in Schedule 1 or any other address (including a facsimile number) notified to the other party in writing in accordance with this clause as an address to which notices, invoices and other documents may be sent. The notice, demand or communication will be deemed to have been duly served:

37.1 if delivered by hand, at the time of delivery;

37.2 if delivered by post, 48 hours after being posted or in the case of Airmail 14 days (excluding Saturdays, Sundays and public holidays) after being posted; or

37.3 if delivered by facsimile, at the time of transmission, provided that a confirming copy is sent by first class post to the other party within 24 hours after transmission.

38. ENTIRE AGREEMENT

38.1 Subject to Clause 38.2, this Agreement and any relevant Call-Off Contract and all documents referred to in this Agreement and any relevant Call-Off Contract, contain all of the terms which the Parties have agreed relating to the subject matter of this Agreement and such documents and supersede and extinguish any prior drafts, agreements, undertakings, representations, warranties and arrangements of any nature whatsoever, whether or not in writing relating to the provision of the

Services. Neither Party has been induced to enter into this Agreement by a statement which it does not contain.

38.2 Nothing in this Clause 38 excludes any liability which one Party would otherwise have in respect of any statement it has made fraudulently to the other Party.

39. RELATIONSHIP OF THE PARTIES

Nothing in this Agreement or any Call-Off Contract constitutes, or shall be deemed to constitute, a partnership between the Parties. Except as expressly provided in this Agreement and any Call-Off Contract, neither Party shall be deemed to be the agent of the other, nor shall either Party hold itself out as the agent of the other.

40. FURTHER ASSURANCE

Each Party will do or procure the doing of all acts and things and execute or procure the execution of all such documents as the other Party reasonably considers necessary to give full effect to the provisions of this Agreement and any relevant Call-Off Contract.

41. GOVERNING LAW

The Agreement shall be governed by and construed in accordance with the law of England and Wales. Without prejudice to Clause 27, the courts of England will have exclusive jurisdiction to settle any dispute which may arise out of or in connection with this Agreement.

THIS AGREEMENT has been signed for and on behalf of the Parties the day and year written above.

Signed by
for and on behalf of
Transport for London

Signature Print name and position

Date:

Signed by
for and on behalf of
Telefónica O2 UK Limited

Signature Print name and position

Date:

SCHEDULE 1 - KEY AGREEMENT INFORMATION

1. Agreement Reference Number: ITC10686

2. Name of Service Provider: Telefónica O2 UK Limited

3. Agreement Commencement Date: 26th March 2009

4. Term: Four (4) Years from the Agreement Commencement Date

5. Details of the Procurement Manager

Name: **Chris Rawson – Vendor Manager**
Address: Windsor House
42- 50 Victoria Street
London SW1H 0TL
Tel: 020 7126 4373
Fax: **Email:** **chris.rawson@tube.tfl.gov.uk**

6. Service Provider's Key Personnel:

Name & Position	Contact Details	Area Of Responsibility
Mark Crossley Account Director	07710 346565	Account/Contract Management
Vickie Noble Service Relationship Manager	07843 092844	Service

7. Additional insurance (if any) to be held by Service Provider:

a) Employer's liability insurance to be £5 million per incident as stated in Clause 21;

b) Public liability insurance to be £10 million per occurrence with financial loss extension;

c) Professional indemnity insurance to be £5 million in the aggregate per annum for the duration of the Call-Off Contract/ Agreement and for 6 years after expiry or termination of the Call-Off Contract/Agreement; and

d) Product liability insurance to be £10 million in the aggregate per annum with financial loss extension.

8. Notice period in accordance with Clause 28.4 (termination without cause): 90 days

9. Address for service of notices and other documents in accordance with Clause 36:

For TfL: Windsor House
42 – 50 Victoria Street
London
SW1H 0TL

Facsimile number: 020 7126 4517

For the attention of: Stephen Kelsey - Procurement Manager

For the Service Provider:
Telefónica O2 UK Limited
Bid Management, Suite G
Arlington Business Centre
Millshaw Park Lane
Leeds
West Yorkshire
LS11 0NE

SCHEDULE 2 - SPECIAL CONDITIONS

In addition to the terms and conditions detailed in clauses 1 to 41 of this Agreement the following Special Conditions are applicable to this Agreement and each Call-Off Contract.

A1 Data Protection

"Data Subject"	has the meaning given to it by section 1(1) of the DPA;
"DPA"	the Data Protection Act 1998;
"Personal Data"	has the meaning given to it by section 1(1) of the DPA;
"Processing"	has the meaning given to it by section 1(1) of the DPA and **"Process"** and **"Processed"** will be construed accordingly;
"Sensitive Personal Data"	has the meaning given to it by section 2 of the DPA;
"TfL Personal Data"	Personal Data Processed by the Service Provider on behalf of TfL;

A1.1 Without prejudice to the generality of Clause 24, the Service Provider shall:

A1.1.1 take appropriate technical and organisational security measures, including as specified in Schedule 9 against unauthorised or unlawful Processing of TfL Personal Data and against accidental loss, destruction of, or damage to such Personal Data;

A1.1.2 provide TfL with such information as it may reasonably from time to time require to satisfy itself of compliance by the Service Provider with Clause A1.1.1;

A1.1.3 co-operate with TfL in complying with any subject access request made by any Data Subject pursuant to the DPA and/or responding to any enquiry made or investigation or assessment of Processing initiated by the Information Commissioner in respect of any TfL Personal Data;

A1.1.4 when notified by TfL, comply with any agreement between TfL and any Data Subject in relation to any Processing which causes or is likely to cause substantial and unwarranted damage or distress to such Data Subject, or any court order requiring the rectification, blocking, erasure or destruction of any TfL Personal Data;

A1.1.5 take reasonable steps to ensure the reliability of personnel having access to TfL Personal Data and to ensure that such personnel are fully aware of the measures to be taken and the Service Provider's obligations under this Clause A1 when Processing TfL Personal Data; and

A1.1.6 not Process any TfL Personal Data outside the European Economic Area (or any country deemed adequate by the Commission pursuant to Article 25(6) Directive 95/46/EC) without TfL's prior written consent.

A1.1.7 ensure that all TfL Personal Data is removed from the Products prior to the Products being recycled or re-used by the Service Provider.

A1.2 When the Service Provider receives a written request from TfL for information about, or a copy of, TfL Personal Data, the Service Provider shall supply such information or data to TfL within such time and in such form as specified in the request (such time to be reasonable) or if no period of time is specified in the request, then within 10 Business Days from the date of the request.

A1.3 TfL remains solely responsible for determining the purposes and manner in which TfL Personal Data is to be Processed. The Service Provider shall not share any TfL Personal Data with any sub-contractor or third party unless there is a written contract in place which requires the sub-contractor or third party to:

A1.3.1 only Process TfL Personal Data in accordance with TfL's instructions to the Service Provider; and

A1.3.2 comply with the same obligations with which the Service Provider is required to comply with under this Clause A1.

A2 IT Systems

"e-GIF"	the UK Government's "e-government inter-operability framework" standard, as may be updated from time to time, details of which are available on the Cabinet Office website, ww.govtalk.gov.uk;
"Euro Compliant"	that the software, electronic or magnetic media, hardware or computer system (whichever is applicable) is capable of, and will not require any replacement or changes in order to be capable of, supporting the introduction of, changeover to and operation of the Euro as a currency and in dual

currency (Sterling and Euro) and will not manifest any material error nor suffer a diminution in performance or loss of functionality as a result of such introduction, changeover or operation and it shall (if applicable) be capable of processing transactions calculated in Euros separately from or in conjunction with other currencies and is capable of complying with any legislative changes relating to the Euro;

A2.1 The Service Provider shall ensure that and in respect of Clause A2.1.1.4 use reasonable endeavours to ensure that:

A2.1.1 any software, electronic or magnetic media, hardware or computer system used or supplied by the Service Provider as part of the Products or Services in connection with this Agreement shall:

A2.1.1.1 not have its functionality or performance affected, or be made inoperable or be more difficult to use by reason of any date related input or processing in or on any part of such software, electronic or magnetic media, hardware or computer system;

A2.1.1.2 not cause any damage, loss or erosion to or interfere adversely or in any way with the compilation, content or structure of any data, database, software or other electronic or magnetic media, hardware or computer system used by, for or on behalf of TfL and/or any other member of the TfL Group, on which it is used or with which it interfaces or comes into contact provided that TfL has complied with any instructions in the use of the above provided by the Service Provider; a

A2.1.1.3 be compliant with e-GIF (including without limitation Table 8 of e-GIF) to the extent that as at the Agreement Commencement Date e-GIF provides that such Products or Services or part thereof are required to be e-GIF compliant and that any Products or Services or part thereof which are not compliant as at the Agreement Commencement Date would become compliant as and when it is a requirement of e-GIF; and

A2.1.1.4 be Euro Compliant; and

any variations, enhancements or actions undertaken by the Service Provider in respect of such software, electronic or

magnetic media, hardware or computer system shall not affect the Service Provider's compliance with this Clause A2.

A4 Infringement of Intellectual Property Rights

A4.1 The Service Provider shall:

A4.1.1 promptly notify TfL upon becoming aware of an infringement or alleged infringement or potential infringement of any Intellectual Property Right which affects or may affect the provision or receipt of the Products or Services or any Bespoke Products/Services or if any claim or demand is made or action brought for infringement or alleged infringement of any Intellectual Property Right; and

A4.1.2 indemnify, keep indemnified and hold harmless TfL from and against all actions, claims, demands, costs, charges or expenses (including legal costs on a full indemnity basis) that arise from or are incurred by TfL by reason of any infringement or alleged infringement of any Intellectual Property Rights of any person arising out of the use by TfL of the Products (or any of them) Bespoke Products/Services or anything arising from the provision of the Services and from and against all costs and damages of any kind which TfL may incur in or in connection with any actual or threatened proceedings before any court or arbitrator. This indemnity does not apply to the extent such actions, claims, demands, costs, charges or expenses are directly caused by TfL's failure to comply with the terms of this Agreement.

A4.2 TfL shall, at the request of the Service Provider, give the Service Provider all reasonable assistance for the purpose of the Service Provider contesting any such claim, demand, or action referred to in Clause A4.1.1 and the Service Provider shall:

A4.2.1 reimburse TfL for all costs and expenses (including legal costs) incurred in doing so;

A4.2.2 conduct at its own expense all litigation and/or negotiations (if any) arising from such claim, demand or action; and

A4.2.3 consult with TfL in respect of the conduct of any claim, demand or action and keep TfL regularly and fully informed as to the progress of such claim, demand or action.

A4.3 If a claim or demand is made or action brought to which Clause A4.1 applies or in the reasonable opinion of the Service Provider is likely to be made or brought, the Service Provider may, after consultation with TfL, at its own expense and within a reasonable time, modify or substitute any or all of the

Products so as to avoid the infringement or the alleged infringement, provided that the terms of this Agreement shall apply mutatis mutandis to such modified or substituted Products and such Products are accepted by TfL.

A5 Specific LU Standards

In this clause, unless the context indicates otherwise the following expressions shall have the following meanings:

"London Underground" the stations and depots, assets, systems, track and other buildings which are used in the maintenance and provision of underground services known as "London Underground".

"LUL" London Underground Limited.

"**LUL Standards"** the mandatory requirements in force on the London Underground from time to time that the Service Provider must comply with in the provision of the Services, comprising mandatory category 1 standards, applicable LUL rules, procedures, codes, standards and safety agreements in relation to, without limitation, health and safety, environment, security, operational, engineering and ambience standards and other customer service delivery standards (including, without limitation, the Contract QUENSH Conditions).

"Contract QUENSH Conditions" the Quality Environmental Safety and Health Contract Conditions in force and as supplied to the Service Provider by LUL from time to time.

Without prejudice to any other provision of this Agreement:

A5.1 The Service Provider acknowledges its awareness of TfL's statutory duty to provide or secure a safe, economic and efficient public passenger transport services by railway for Greater London and shall at all times during this Contract have regard to TfL's statutory duties. The Service Provider shall not, in the performance of the Services, in any manner endanger the safety of or interfere with the operation of the Underground Network or endanger the public and shall minimise any disruption to both the Underground Network and the public, and

A5.2 The Service Provider acknowledges, and undertakes to inform all its employees, agents and subcontractors who will be using TfL's communication facilities that TfL reserves the right from time to time to:

A5.2.1 intercept, for the purposes of monitoring and / or recording, any communication made through any system capable of transmitting communications including but not limited to

telephone, electronic mail, facsimile, voicemail or internet facility provided by TfL; and

A5.2.2 use any information obtained as a result of any intercepted communication referred to in Clause A5.2.1 for the purposes permitted by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

A5.3 In providing the Services, the Service Provider shall comply with LUL Standards.

A5.4 One of the LUL Standards which may be of relevance to this Agreement is QUENSH which governs safety for places of work on or around the operational railway. If relevant, the Service Provider shall be required to comply with LUL's Contract QUENSH Conditions as indicated and respond to the menu provided by the Procurement Manager.

A5.5 It is the responsibility of the Service Provider to ensure that it receives the LUL Standards from LUL for the required Services and must ensure that it has been appraised by LUL as capable of providing the Services in terms of the LUL Standards. If the Service Provider has not been appraised or has not been provided with the Contract QUENSH Conditions, it is the Service Provider's obligation to raise this with the Procurement Manager and if necessary cease work until the appraisal is completed.

A5.6 Where there is a requirement indicated in the Contract QUENSH Conditions to comply with one or more conditions, it is the responsibility of the Service Provider to satisfy itself of the requirements of the indicated conditions as contained in Contract QUENSH Conditions Standard. Access to LUL Standards can be gained through the intranet, which access can be obtained on request through the Contract Manager.

A6 Provision and Use of Products and Services

"Accessories"	means items for use in conjunction with a Device including but not limited to batteries, chargers, headsets, USB cables and laptops;
"Age Restricted Service"	means any services which are specified for use only by a person over a specific age;
"Airtime"	means wireless network capacity ordered by TfL and provided by the Service Provider, and which includes GPRS Bearer;
"Content"	information, communications, images and sounds, video, games including any associated software, or any other material contained on or available through the Services;
"Coverage Area"	means the area, location, or place, as identified in the Technical Requirements Specification within which the Services shall be provided to TfL by the Service Provider which area, location, or place may be enhanced, or increased from to time;
"Device"	means a Product which is a mobile telephone or other wireless device incorporating a SIM Card and used for the transmission and receipt of voice and/or data;
"End User"	any individual user of the Services;
"GPRS Bearer"	means the General Packet Radio Service provided by the Service Provider;
"Media"	means Content, Service Provider Software and Third Party Software;
"Network"	means the electronic communications network through which the Service Provider provides (or procures the provision of) the Services;
"Number"	means a telephone number allocated to TfL by the Service Provider;
"Roaming"	means the facility whereby TfL can use a Device in conjunction with a network which is not the Network;
"Service Provider Software"	means any software owned by or licensed to the Service Provider and supplied to TfL under the

terms of this Agreement;

"SIM Card"	means the subscriber identity module supplied by the Service Provider (which shall at all times during the Term remain the property of the Service Provider) which is allocated to TfL for use with a Device and which contains a Number;
"TfL Products"	means any Devices and/or SIM Cards not supplied by the Service Provider under the terms of the Framework Agreement and notified by TfL to the Service Provider as being required for connection to the Network;
"Third Party Software"	means any software which is not Service Provider Software;

A6.1 The Service Provider agrees during the Term to:

A6.1.1 connect and activate each SIM Card provided to TfL to enable the receipt of the Services by End Users and the Service Provider shall allocate Numbers appropriately to each SIM Card;

A6.1.2 procure that any TfL Products are connected to the Network for the provision of the Services except where the same cannot be achieved for technical reasons;

A6.1.3 use all reasonable endeavours to make the Services available in the Coverage Area at all times; and

A6.1.4 subject to A6.2 below, provide or procure the provision of Airtime on a 24 hours a day 365 days per year basis.

A6.2 TfL accepts that in relation to some of the Services which are concerned with the transmission and/or receipt of electronic communications signals (including without limitation the provision of Airtime), it is technically impracticable to provide a fault-free service and the Service Provider does not undertake to do so. Further, TfL acknowledges that the provision of Airtime is subject to the geographic extent of Airtime coverage and local geography, topography and/or atmospheric conditions and/or other physical or electromagnetic interference and/or the number of users trying to access the Wireless Services in any particular location that may from time to time adversely affect the provisions of the Airtime in terms of availability, line clarity and call interference.

A6.3 Subject to Clauses A6.2, A6.8 and A6.9, the Coverage Area may only be reduced or decreased at any time:

A6.3.1 in accordance with in terms of Clause 33 of the Framework Agreement; or

A6.3.2 if required by a competent regulatory authority.

Further the Parties acknowledge that from time to time there may be interference or a decrease in small areas of the coverage Area due to construction developments and in such event the Service Provider shall keep TfL informed of any such decreases and will use all reasonable endeavours to ensure that the coverage Area is increased as soon as reasonably possible.

A6.4 If the Coverage Area is reduced or decreased at any time as specified in Clause A6.3, TfL shall have the right, at its option, to either:

A6.4.1 deal with such reduction or decrease as a variation in accordance with Clause 33 of the Framework Agreement; or

A6.4.2 terminate the relevant Call-Off Contract pursuant to Clause 28 of the Framework Agreement.

A6.5 TfL shall be permitted to use the Services from the Service Commencement Date provided always that:

A6.5.1 it complies with any reasonable instructions notified in writing from time to time to TfL by the Service Provider relating to the proper and effective use, or provision of, the Services;

A6.5.2 it does not use (or permit the use) of Services:

A6.5.2.1 in any way which is fraudulent, improper, immoral or unlawful, or to the knowledge of TfL has any fraudulent, improper, immoral or unlawful purpose or effect, including to transmit, knowingly receive, store, upload, download, use or re-use any material which is abusive, indecent, defamatory, obscene or menacing; or

A6.5.2.2 to obtain access, through whatever means, to notified restricted areas of the Network; or

A6.5.2.3 to send unsolicited communications; or

A6.5.2.4 to cause annoyance, inconvenience or anxiety;

A6.5.3 it agrees (where necessary) to enter into an end-user licence agreement with the owner of copyright in the Service Provider Software or any Third Party Software provided as part of the Services;

A6.5.4. it does not knowingly or recklessly use the Services in a manner which infringes, or may infringe, the rights of a third party (including Intellectual Property Rights and any privacy rights);

A6.5.5 it agrees to meet any minimum specifications for handheld PC operating systems and laptop PC operating systems as set out by the Service Provider, as available in hard copy upon request;

A6.5.6 it will procure that any TfL Products to be connected to the Network pursuant to Clause A6.1.2 are suitable for use in conjunction with the Services;

A6.5.7 it does not use the Services in a way which (in the reasonable opinion of the Service Provider) brings the name of the Service Provider into disrepute or which places the Service Provider in breach of any laws;

A6.5.8 it does not use the Services for the purpose of marketing or advertising products or services (including the Services) to End Users without their consent;

A6.5.9 it complies with any fair use restrictions enforced by the Service Provider provided that the same have been notified to TfL in writing prior to the commencement of the relevant Call-Off Term; and

A6.5.10 it does not send any Content which is offensive, abusive, indecent, defamatory, obscene or menacing, a nuisance or a hoax.

A6.6 The Service Provider can at its discretion suspend any SIM Card from making calls (other than to the emergency services) and disconnect any SIM Card from the Services if the Service Provider has reasonable cause to suspect fraudulent use of the SIM Card or the Device, or either are notified by TfL as being stolen.

A6.7 The Service Provider may (having given as much notice to TfL as possible) suspend some or all of the Services:

A6.7.1 if the Service Provider is required to do so by the emergency services or other governmental authority;

A6.7.2 if the Service Provider has good reason to believe that a Device or the Services are being used in breach of Clause A6.5.2 above.

A6.8 The Service Provider may at any time (and, where reasonably practicable, with prior written notice to TfL) make such minor technical or other alterations to the Services as it in its reasonable opinion deems necessary (including without limitation to safeguard the integrity and security of the Network) provided always that such alterations do not materially adversely affect TfL's use of the Services.

A6.9 The Service Provider shall use reasonable endeavours to ensure that Roaming services are provided to an equivalent level with the provision of Services under this Agreement.

A6.10 TfL may replace a Device in use by purchasing another device ("Upgrade") at the price set out in Schedule 6 of the Framework Agreement or, if not specified, at the Service Provider's then up to date list price.

A6.11 The Service Provider shall connect any Upgrades for the remainder of the relevant Call-Off Term.

A6.12 TfL acknowledges that:

A6.12.1 each SIM Card is capable of receiving text messages and other Content from sources other than the Service Provider and the Service Provider shall not be liable for Direct Losses arising from the receipt of such text messages and Content; and

A6.12.2 the Service Provider is acting as a service provider and as such, has no knowledge of, involvement with, or liability for specific content of any text messages or other Content sent by TfL.

A6.13 The Service Provider may make Media available to TfL and End Users whether as part of the provision of Services or by virtue of use of the Services and all such Media is subject to the terms of this Clause A.6.

A6.14 TfL shall not:

A6.14.1 copy, modify, store, forward, publish or distribute any Media without permission of the Service Provider or the relevant rights owners;

A6.14.2 use Media other than for TfL's internal use and not for any commercial purpose or distribution to any third party (unless expressly permitted by the terms upon which such Media has been provided); and

A6.14.3 not circumvent any Age Restricted Service or digital rights management mechanisms.

A7 VPN Access

"VPN" means a virtual private network.

A7.1 The Service Provider shall, in accordance with the Technical Requirements Specification, provide data access Services allowing TfL's Devices to connect to, and transmit data across the Internet, and to connect to its own supplied VPN.

A7.2 In such circumstances, TfL shall (subject to the contrary being provided for in a Call-Off Contract under this Agreement in which case such Call-Off Contract shall take precedence) be responsible for:

A7.2.1 selecting, sourcing, installing, configuring and maintaining, at its own cost, any necessary equipment and infrastructure for the purpose of ensuring that End Users may access TfL's VPN in accordance with TfL's own usage and security policies; and

A7.2.1 ensuring that any such equipment and infrastructure is compatible with the Network and adheres to any technical parameters and guidance issued by the Service Provider from time to time provided that the same shall be made available to TfL on request.

A8 Regulatory Compliance

"General Conditions of Entitlement"	means the general conditions notified by the Director General for Telecommunications under section 45 of the Communications Act 2003 as amended (and a "General Condition" shall be construed accordingly);
"Location Data"	has the meaning given to that expression in the Privacy and Electronic Communication (EC Directive) Regulations 2003;
"Number Portability"	has the meaning given to that expression in General Condition 18 of the General Conditions of Entitlement;
"PATS Service"	means a Publicly Available Telephone Service as defined in Part 1 of the General Conditions of Entitlement;
"Traffic Data"	has the meaning given to that expression in the Privacy and Electronic Communication (EC Directive) Regulations 2003;
"Value Added Service"	has the meaning given to that expression in the Privacy and Electronic Communication (EC Directive) Regulations 2003;
"WEEE Equipment"	means any Products which fall within the scope of the WEEE Regulations;
"WEEE Regulations"	means the Waste Electrical and Electronic Equipment Regulations 2006 (as amended);

A8.1 The Service Provider shall ensure that the performance of its obligations under this Agreement (including ensuring that the Products and Services) comply at all times during the Term with the requirements of any applicable Laws (including, without limitation, the Communications Act 2003, the General Conditions of Entitlement and, in relation to Products, the WEEE Regulations, the Restriction of the Use of Certain Hazardous Substances in the Electrical and Electronic Equipment Regulations 2008, and relevant to the Services, the Service Provider's business and/or TfL's business from time to time in force, which are or become applicable to the Services, the Service Provider's obligations under this Agreement.

A8.2 Where any Service provided by the Service Provider is or becomes a PATS Service, the Service Provider shall take all necessary steps to comply with the General Conditions which apply to the provision of a PATS Service, and TfL will comply fully with the Service Provider to achieve such compliance.

A8.3 The Service Provider shall not without the prior written consent of TfL use Traffic Data and/or Location Data for the provision of Value Added Services for any third party other than TfL Group.

A8.4 In exceptional cases, a regulatory authority may require the re-allocation or change of telephone numbers in which case the Service Provider reserves the right to change any Numbers effected by such a change, provided always that the Service Provider shall make such representations to the regulatory authority as are required to avoid such number changes and in the event that such number changes are implemented by the regulatory authority, the Service Provider will take all reasonable steps to mitigate the cost to TfL of resulting changes to Numbers.

A8.5 The Service Provider shall, following termination of this Agreement and a request in writing by TfL, provide Number Portability to TfL and TfL shall pay any reasonable charges incurred by the Service Provider in providing such Number Portability.

A8.6 When procuring any WEEE Equipment for use in accordance with this Agreement whether by direct purchase by the Service Provider, purchase on behalf of TfL, lease or otherwise, the Service Provider shall ensure that in accordance with the WEEE Regulations that the producer of the WEEE Equipment (whether that be the Service Provider or a third party) shall assume responsibility for financing the costs of the collection, treatment, recovery and environmentally sound disposal of:

A8.6.1 all WEEE arising from the WEEE Equipment; and

A8.6.2 all WEEE arising from equipment placed on the market prior to 13 August 2005 where such equipment is to be replaced by the WEEE Equipment and the WEEE Equipment is of an equivalent type or is fulfilling the same function as the equipment.

A8.7 The Service Provider shall indemnify, keep indemnified, and hold TfL harmless from and against any and all losses, costs or expenses which TfL incurs as a result of any failure on the part of the Service Provider or the relevant producer to comply with the terms of Clause A8.6.1.

A8.8 The Service Provider shall bear the cost of compliance with any amendments to, re-enactments of, superseding of and/or replacement of laws in accordance with the allocation of cost provisions set out in this Clause A.8 except that where any such amendment necessitates a change to the Services as specified in a Call-Off Contract and provided that such amendment could not have reasonably been foreseen by the Service Provider at the date of this Agreement, the Parties shall enter into good faith negotiations to make such adjustments to the Charges as may be necessary to compensate the Service Provider for such additional costs as are both reasonably and necessarily incurred by the Service Provider in accommodating such amendments.

A9 Ethical Sourcing Terms and Conditions

A9.1 TfL is committed to ensuring that workers employed in its supply chains throughout the world are treated fairly, humanely and equitably. In the course of complying with this Agreement, the Service Provider shall comply with and shall procure that its sub-contractors (as applicable) comply with those principles of the Ethical Trading Initiative (ETI) Base Code as are detailed in Appendix 1 to these Special Conditions, or an equivalent code of conduct (the "Ethical Sourcing Principles") in relation to the provision of the Products and Services.

A9.2 As soon as practicable following the Agreement Commencement Date the Service Provider shall be registered with an ethical supplier database, such as SEDEX (Supplier Ethical Data Exchange). The Service Provider agrees that for the duration of this Agreement, it shall permit and enable TfL to have access to the information relating to the Service Provider that subsists in such ethical supplier database.

A9.3 During the course of this Agreement, TfL has the right to request the Service Provider to carry out one or more audit using a reputable auditor to verify whether the Service Provider is complying with the Ethical Sourcing Principles. The identity of the auditor is to be approved by TfL, such approval not to be unreasonably withheld or delayed. The costs of the audit shall be borne by TfL.

A9.4 During the course of this Agreement, if TfL has reasonable cause to believe that the Service Provider is not complying with any of the Ethical Sourcing Principles, then TfL shall notify the Service Provider and the Parties shall agree an action plan with appropriate timeframes for compliance by the Service Provider (the "Action Plan"), such Action Plan to be agreed by the Parties by no later than [insert timeline] from the date of TfL notifying the Service Provider that remedial action is required or such other period as the

Parties may otherwise agree in writing. The costs of the creation and implementation of the Action Plan shall be borne by the Service Provider.

A9.5 Following the agreement of the Action Plan, TfL reserves the right to conduct one or more audits, (either itself or via a third-party auditor approved by TfL) in relation to compliance by the Service Provider with the Action Plan.

A9.6 For the avoidance of doubt, the rights of audit contained in this clause A9.6 shall include without limitation the right of TfL (or a TfL-approved auditor) acting reasonably to undertake physical inspections of relevant sites/factories, to conduct interviews with relevant personnel and to inspect relevant documents. The Service Provider shall co-operate and shall procure that its sub-contractors (as applicable) co-operate with TfL in relation to all aspects of any audit.

A10 Environmental and Social Responsibility

The Service Provider shall carry out it's obligations under this Agreement in respect of environmental and social responsibility which includes those that are detailed on the Service Providers website via the link http://www.Service Provider .com/cr/operating_responsibly.aspand such obligations shall be in accordance with all applicable quality assurances, and includes obligations in respect of the recycling of mobile devices at end of life.

APPENDIX 1: THE ETI BASE CODE

1.1 EMPLOYMENT IS FREELY CHOSEN

1.1.1 There is no forced, bonded or involuntary prison labour.

1.1.2 Workers are not required to lodge "deposits" or their identity papers with their employer and are free to leave their employer after reasonable notice.

1.2 Not used

1.3 WORKING CONDITIONS ARE SAFE AND HYGIENIC

1.3.1 A safe and hygienic working environment shall be provided, bearing in mind the prevailing knowledge of the industry and of any specific hazards. Adequate steps shall be taken to prevent accidents and injury to health arising out of, associated with, or occurring in the course of work, by minimising, so far as is reasonably practicable, the causes of hazards inherent in the working environment.

1.3.2 Workers shall receive regular and recorded health and safety training, and such training shall be repeated for new or reassigned workers.

1.3.3 Access to clean toilet facilities and to potable water, and, if appropriate, sanitary facilities for food storage shall be provided.

1.3.4 Accommodation, where provided, shall be clean, safe, and meet the basic needs of the workers.

1.3.5 The company observing the code shall assign responsibility for health and safety to a senior management representative.

1.4 CHILD LABOUR SHALL NOT BE USED

1.4.1 There shall be no new recruitment of child labour.

1.4.2 Companies shall develop or participate in and contribute to policies and programmes which provide for the transition of any child found to be performing child labour to enable her or him to attend and remain in quality education until no longer a child.

1.4.3 Children and young persons under 18 shall not be employed at night or in hazardous conditions.

1.4.4 These policies and procedures shall conform to the provisions of the relevant LOI standards.

1.5 LIVING WAGES ARE PAID

1.5.1 Wages and benefits paid for a standard working week meet, at a minimum, national legal standards or industry benchmark standards, whichever is higher. In any event wages should always be enough to meet basic needs and to provide some discretionary income.

1.5.2 All workers shall be provided with written and understandable Information about their employment conditions in respect to wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid.

1.5.3 Deductions from wages as a disciplinary measure shall not be permitted nor shall any deductions from wages not provided for by national law be permitted without the expressed permission of the worker concerned. All disciplinary measures should be recorded.

1.6 WORKING HOURS ARE NOT EXCESSIVE

1.6.1 Working hours comply with at least UK national laws and benchmark industry standards, whichever affords greater protection.

1.6.2 Not used.

1.7 NO DISCRIMINATION IS PRACTISED

1.7.1 There is no discrimination in hiring, compensation, access to training, promotion, termination or retirement based on race, caste, national origin, religion, age, disability, gender, marital status, sexual orientation, union membership or political affiliation.

1.8 REGULAR EMPLOYMENT IS PROVIDED

1.8.1 To every extent possible work performed must be on the basis of recognised employment relationship established through national law and practice.

1.8.2 Obligations to employees under labour or social security laws and regulations arising from the regular employment relationship shall not be avoided through the use of labour-only contracting, sub- contracting, or home-working arrangements, or through apprenticeship schemes where there is no real intent to impart skills or provide regular employment, nor shall any such obligations be avoided through the excessive use of fixed-term contracts of employment.

1.9 NO HARSH OR INHUMANE TREATMENT IS ALLOWED

1.9.1 Physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation shall be prohibited.

SCHEDULE 3 - PRODUCTS AND SERVICES

1. Introduction

This Schedule details the scope of the Products and Services.

The scope of the procurement of the Products and Services can be summarised as mobile services to meet TfL's current and evolving requirements for enterprise mobile telecoms over the duration of this Agreement. The Services are categorised as:

- Corporate mobile telephony and email –enterprise-wide provision of handsets and mobile email / data devices, line rental, airtime and associated accessories;
- Corporate mobile data solutions – network access and "airtime" to support specific business applications deployed on mobile devices;
- Potentially where feasible, provision of those mobile data applications; and
- Corporate wireless infrastructure solutions – provision of infrastructure to support the above services.

The scope of these Services is detailed in the following sub-sections.

To remove ambiguity, services explicitly excluded from the scope are detailed in section 7.

2. Corporate Mobile Telephony and Email

- Provision of equipment to access a national public wireless network (this includes handsets, SIM cards and accessories); and
- Provision of line rental and "airtime" including voice calls, short messaging and packet data services;
- Provision of a fully managed mobile email solution.
- Provision of a mobile email solution for Surface staff (originally via the "Flexiworker project") using a push email solution. This is provided via access to TfL's MS Exchange infrastructure from Windows Mobile devices. This also includes "Cognito" messages (see section 3 below).
- Provision of a paging service for TfL including pagers and a desktop application.
- Group / Bulk SMS –
- Code 5 – a personal safety service, currently provided by Orbis, for Surface revenue protection staff. In a personal safety emergency, the user dials 5 on their mobile phone / device; the call is then routed directly to the system provider who will locate the user and provide assistance.

TfL's requirements for corporate mobile telephony and email services are not likely to substantially change over the duration of this Agreement, although TfL will require

the flexibility to deploy the most appropriate solution to users based on the business requirement.

3. Corporate Mobile Data Solutions

A number of existing TfL applications and systems transmit data to and from mobile devices, usually via a cellular network. These have been selected and/or developed to respond to a particular business need, and have typically been procured / developed at a business unit level. They vary from small applications developed in-house, to off the shelf applications, or bespoke turn-key solutions delivered by a solution integrator.

For the purposes of this Agreement, it is necessary to distinguish applications from the client device, and the network element of each mobile data solution.

- The **application** shall refer to the specific mobile data software that has typically been developed to meet the specific business need.
- The **device** shall refer to the piece of user hardware that the software operates on. For a mobile solution, this is typically a handset.
- The **network** provides the raw data connectivity to enable the application to communicate with other devices. For a corporate mobile data solution, this is typically a wireless network which is connected to the fixed corporate network. This gives the mobile application access to resources (e.g. application servers) within the corporate network.

TfL believe it will benefit from establishing a strategic relationship with a supplier at a group-wide level to deliver the network element, the devices and potentially the mobile applications as a managed service. The provision of each application will be considered on a case by case basis.

The mobile devices and the network connectivity delivered by the Service Provider will need to be compatible with all mobile data applications that are currently in existence across TfL's mobile estate.

TfL would like to explore opportunities to migrate the mobile services (potentially including the applications) to a single supplier *where it is beneficial and contractually allowable to do so*, introducing economies of scale, improving technical and cost efficiency, and thereby ensuring best value is obtained for the mobile services. As a result, TfL anticipates that the Service Provider will need to partner with TfL's existing application providers to provide and manage the mobile data applications under this framework agreement.

In certain cases, the mobile data applications shall not be in scope, although the network elements (i.e. the data connectivity), and the device shall be in scope. For example, this may be the case where the mobile element forms part of a wider project and it would not be suitable for the entire project / solution to be delivered under the Mobile Services agreement. An example of where this would be the case is the Future Ticketing Project. The existing and identified mobile data solutions identified above shall be provided under the terms of this Agreement as optional

Call-Offs under a Call-Off Contract. TfL expect future mobile service requirements of a similar nature to be included in the scope of this Agreement.

Where the existing application cannot be supported, or additional benefit can be realised, TfL would expect suppliers to suggest equivalent, alternative applications / solutions.

The following existing internal mobile data solutions (i.e. not public-facing) are considered in-scope for this procurement as detailed below:

- Cognito – a remote data capture system used by TfL's Transport Policing and Enforcement Directorate (TPED) and London Buses Network Operations (for instance to issue penalty fares). The Cognito system is currently based on a Windows Mobile PDA and GSM / GPRS / UMTS data which interfaces with a Bluetooth printer for ticket issue. For this solution, only the device, network access and data transfer elements are in scope. Cognito Ltd. will continue to deliver the application.
- AMT Sybex – a mobile data system used by TPED and the Metropolitan Police in patrolling "red routes" for example for the issue of parking tickets. The AMT Sybex system is currently based on a Windows Mobile PDA and GSM / GPRS data. For this solution, only the device, network access and data transfer elements are in scope. AMT Sybex will continue to deliver the application.
- QSI (Quality of Service Indicators) – a mobile data system used by TfL's Surface Information Management for monitoring and reporting bus movements. This system is developed and managed in-house and is currently based on a Windows Mobile PDA and GSM / GPRS data over the APN. For this solution, only the device, network access and data transfer elements are in scope.
- Confirm Phase 2 – a workforce and workflow management system currently under development for London Buses Infrastructure Development for the management and maintenance of bus infrastructure (i.e. bus stops etc.). This is based on a Windows Mobile device and uses the existing "Cognito" APN link.
- Real-Time Service Information – a mobile data system used by London Underground station staff for real-time service information via the intranet. This service is based on a BlackBerry handset.
- Mobile applications that enable IT service management information to be accessed and updated from mobile devices (currently BlackBerrys) by integrating with TfL's Remedy service management system.
- PCO – a small application for the Public Carriage Office to perform vehicle registration queries. This is currently based on a Windows Mobile PDA and GSM / GPRS / UMTS data.
- Scisys – a remote data capture system for London Underground for revenue collection staff, based on a BlackBerry device.

- Incident Management System, location service – a service used by Surface within their Emergency Control Centre to locate corporate mobile users using cell / base station information. This uses the existing Surface APN.

Additionally, a number of future projects across TfL will feature an element of mobile services, and therefore may be called-off under a Call-Off Contract from this Agreement in due course. Those which are currently identified are summarised below, although may be subject to change:

- Future Ticketing Project – a replacement to the existing "Oyster" platform will be delivered by 2011; the project is currently at the concept phase.

  Every Oyster reader will require real-time communications to a database of ticketing information, including allowed and blocked cards; the maximum round-trip time will be approximately 700ms. For buses in particular, it is currently envisaged that a local database instance will be required in each bus, and this database will need to be updated as often as possible (potentially every 10 minutes) via the wireless network.

  Alternatively, the transaction could happen in real time using the wireless network if network characteristics allowed the round-trip time to be less than 700ms, and network availability (both geographical and time) was near 100%.

  In addition, handheld units used by revenue enforcement officers will require similarly up-to-date information. This update may be provided via the cellular network, or potentially via a wireless interface with the vehicle unit.

4. Corporate Wireless Infrastructure Solutions

The Service Provider shall provide infrastructure to support the mobile services detailed in the above subsections. Currently this includes:

- BlackBerry Enterprise Server (BES) software and licences to support the existing mobile email services described in section 0 (this forms part of the Blackberry Managed Service);
- Provision of a mobile VPN solution to support the voice and data services to integrate with TfL's fixed telephony and dialling plan, enable "one number" functionality and deliver cheaper "on-net" calls. This should result in reduced costs and increased control of costs; and
- A number of fixed Access Point Name (APN) data links (either private leased line, or VPN) between TfL sites and a wireless network to support the mobile data solutions.
- In each of the above cases, TfL will require the Service Provider to consolidate and rationalise the existing requirements where feasible to improve cost, technical and operational efficiencies.

Additionally, a number of projects across TfL are anticipated which may require elements of corporate wireless infrastructure, and therefore may be included in the scope of services to be potentially provided by the Service Provider under this

Agreement. These are considered by TfL to be aspirational services that may or may not be required over the duration of this Agreement. These are as follows:

- Provision of a fixed-mobile convergence solution to reduce charges for calls that are made and received in TfL buildings and sites and reduce infrastructure costs;
- Provision of private wireless coverage (both voice and data) in underground stations to support station staff, giving them access to real-time information (this may or may not be the fixed-mobile convergence solution above); and
- Potentially, provision of public cellular coverage (both voice and data) across the London Underground network (this may or may not be included with the fixed-mobile convergence solution and private wireless coverage above), although this is to be explored at a strategic level to ensure feasibility.

5. Service Management

TfL require the Services specified in this Agreement to be provided as managed services. However, it is envisaged that specific call-offs from this Agreement may require varying levels of management as some business units may manage the services in-house; these will be specified in the Call-Off Contract.

The Service Provider is required to quote for service management separately as an optional item for each Service.

6. Project Work and Consultancy

Over the duration of this Agreement, TfL envisage that the Service Provider's technical input to specific projects will be required. These projects would typically be to establish new services, and therefore the Service Provider's involvement would not be expected to be performed as part of management of the existing services.

7. Exclusions

To remove ambiguity, related services which are out of scope are detailed below:

- Development and delivery of public-facing mobile applications – this is within scope of a separate project and associated procurement exercise.
- i-Bus – a replacement bus radio system which is currently delivered by a consortium. The mobile service requirements relating to the system are currently assumed as out of scope.
- Private mobile radio services (such as Airwave).

SCHEDULE 4 - NOT USED

SCHEDULE 5 – SERVICE MANAGEMENT REQUIREMENTS

1. Introduction

1.1. The Service Management Requirements relating to the provision of the Services include, but are not limited to, the Services set out in this Schedule. The Service Management Requirements may be added to or amended from time to time by agreement between the parties.

1.2. The following service elements will be available from the Agreement Commencement Date or within a maximum of 6 months from the Agreement Commencement Date.

1.3. The Services have been categorised into the elements of service that shall be available to TfL and those elements which are optional and incur an additional charge. The optional service elements shall be charged in accordance with Schedule 6 or, if the Charges are not set out within Schedule 6, then the Service Provider will provide advance written notice to TfL of the amount of such Charges which will then be agreed between the parties.

2. Standard Service Elements

The following are the 'standard' service elements which shall be available to all parties at no additional charge unless expressly stated otherwise:

2.1. Transition / migration requirements

2.1.1. The Service Provider shall be solely responsible for the migration of mobile services currently operated by other providers, at no cost to TfL.

2.1.2. TfL shall not experience a drop in service levels during the transition of the Services to the Service Provider.

2.1.3. The Service Provider shall be required to consolidate and rationalise the existing mobile services where it is appropriate to do so (e.g. VPN/APN links).

2.1.4. The Service Provider shall identify user accounts with zero voice and data use, investigate and disconnect those accounts where appropriate.

2.2. Capacity Management

2.2.1. The Service Provider is required to manage the capacity of the mobile services to ensure it meets TfL's ongoing requirements.

2.2.2. Capacity management shall include but may not be limited to the following services:

2.2.2.1. Capacity of the wireless network to allow voice services;

2.2.2.2. Capacity of the wireless network to allow data services;

2.2.2.3. Bandwidth of the VPN / APN links for the mobile data applications and mobile VPN services; and

2.2.2.4. Number of users on the Blackberry Enterprise Server.

2.2.3. The Service Provider is required to manage the capacity of the Services stated above to ensure technical and cost efficiency for TfL.

2.2.4. The Service Provider shall identify where capacity exceeds 150% of the peak demand and propose and implement changes (e.g. rationalisation) where they would benefit TfL.

2.2.5. The Service Provider shall be required to consolidate and rationalise the existing mobile services where it is appropriate to do so (e.g. VPN/APN links).

2.2.6. The Service Provider shall identify user accounts with zero voice and data use, investigate and disconnect those accounts where appropriate.

2.3. Incident and Problem Management

2.3.1. The Service Provider will have in place incident and problem management processes and where applicable will integrate with the existing TfL incident management processes.

2.4. Disaster Recovery

2.4.1. Where appropriate, the mobile services are to be provided in a resilient manner as part of their disaster recovery strategy. In particular, this shall apply to the mobile infrastructure elements described in section.

2.5. Change Management

2.5.1. The Service Provider is required to respond to potential changes in this Agreement or the Services delivered under this Agreement, brought on by either party. For instance, these could be:

2.5.1.1. Changes to the Services required by TfL;

2.5.1.2. Changes to the Services to be delivered to TfL;

2.5.1.3. Changes to the service management requirements; and

2.5.1.4. Changes to the commercial arrangements between parties (e.g. costs / tariffs).

2.5.2. TfL shall not experience any interruption in service due to any of the above changes.

2.6. Mobile Service Desk (located at the Service Provider's premises)

2.6.1. The Service Provider shall provide a dedicated mobile service desk to provide a comprehensive support service to TfL users.

2.6.2. The mobile service desk shall be staffed by Service Provider personnel.

2.6.3. The mobile service desk hours of operation shall be 08:00 to 18:00 Monday to Friday.

2.6.4. The service desk shall provide the following services:

Processing and investigating calls relating to faults or problems with the mobile services;

2.6.4.1. Receiving and processing orders for new devices / connections;

2.6.4.2. Receiving and processing orders for upgrade devices;

2.6.4.3. Set-up and configuration of new and upgrade devices;

2.6.4.4. Replacement of faulty devices

2.6.4.5. Recycling or disposal of devices no longer required;

2.6.4.6. Arranging delivery of new and upgrade devices, and collection of faulty devices; and

2.6.4.7. Additional, related services that may be required by TfL over the duration of the contract.

2.6.5. TfL will inform the Service Provider of any change to these requirements.

2.6.6. In addition to the dedicated TfL service desk, the Service Provider shall provide a separate customer service facility available 24 hours a day, 365 days a year to allow cancelling or barring of lost or stolen phones.

2.7. Maintenance and Repair

2.7.1. All mobile devices shall be provided under a 12 month warranty.

2.7.2. The Service Provider shall provide a replacement working device of the same model within 1 working day of the receipt of the request from TfL, provided the order is placed before 12 noon. The replacement shall be delivered to any address of TfL's choice between the hours of 08:00 and 18:00.

2.8. Service Provisioning

2.8.1. New or upgrade handsets and SIM cards shall be supplied within 5 working days of receipt of a valid service request.

2.8.2. The Service Provider shall maintain an appropriate level of stock to meet TfL's demand for new or upgrade handsets. This is dependant on the model required and the stock available to the Service Provider from handset manufacturers.

2.8.3. The Service Provider shall set-up the mobile email service (both BlackBerry and Windows Mobile) for users within 5 working days of a new service request.

2.8.4. The Service Provider shall be required to work with TfL to improve the ordering process that is currently in place.

2.9. User Account Management and Billing

2.9.1. Users shall be able to select paper-based or online account management and billing.

2.9.2. The Service Provider shall provide a solution for users to identify business use from personal use.

2.10. TfL Account Management

2.10.1. The Service Provider shall make available a dedicated account manager who shall act as a single point of contact for the provision of mobile services.

2.10.2. The Service Provider's account manager shall be responsible for:

2.10.2.1. advising TfL of any technical developments or products and services that will or may have an impact on any aspect of the services;

2.10.2.2. providing reports to TfL as specified in this Schedule 5;

2.10.2.3. attending monthly account management meetings;

2.10.2.4. participating in corporate IM service reviews; and

2.10.2.5. ensuring that the Service Provider meets the requirements detailed in this document.

2.10.3. The Service Provider shall make available an account manager for each of the major business units within TfL.

2.11. Service Level Agreements

2.11.1. The Service Provider shall provide the services in accordance with this Schedule 5 and in accordance with any service levels as set out in the applicable Call-Off Contracts.

2.11.2. The Service Provider's network shall have an overall availability of 99%, measured on a monthly basis.

2.12. Service Performance, Management Information and Reporting

2.12.1. The Service Provider shall provide comprehensive management reports on a monthly basis to a nominated TfL representative.

2.12.2. These shall report the current status of the mobile service estate, including the following information:

2.12.2.1. Number of connected devices by type (phone / PDA);

2.12.2.2. Number of active devices of each mobile data application;

2.12.2.3. Total number of calls made over the past month, number of minutes and associated costs;

2.12.2.4. Total number of sent SMS messages and associated costs;

2.12.2.5. Total amount of transferred data and associated costs;

2.12.2.6. Service performance against the Service Level Agreements; and

2.12.2.7. Any other service management information that may be requested by TfL on a regular or one-off basis. Depending on the requirements, there may be an additional charge.

2.12.3. Where relevant, the above information shall be provided in a per-user/device, per-business unit and total basis.

2.12.4. The reports shall contain analysis of usage trends, and highlight where irregular or potentially fraudulent behaviour may be occurring. The reports shall also recommend actions to manage demand and cost.

2.12.5. The Service Provider is required to identify and pro-actively suggest initiatives to improve the efficiency or effectiveness of the mobile services or deliver additional benefits to TfL, to ensure that TfL obtain best value from the mobile services agreement.

2.13. Service Credits

2.13.1. Where Service Credits apply, these shall be calculated in accordance with the relevant Call-Off Contract.

3. Optional chargeable service elements:

The following are the optional chargeable service elements. The Charges for these Services shall be in accordance with Schedule 6 or, where the Charges are not set out in Schedule 6, the Charges will be as agreed between the parties.

3.1. Configuration and Asset Management

3.1.1. The Service Provider shall maintain an asset management database of connected devices, software licences, etc. This shall integrate with the existing TfL Configuration Management Database (CMDB).

3.2. Mobile Application Management

3.2.1. The Service Provider shall manage the subset of mobile data applications which have been identified as in the scope of provision.

3.2.2. Where appropriate and agreed between the Service Provider and TfL, the application management services to be provided shall include but shall not be limited to:

3.2.2.1. Deployment of mobile data applications to mobile devices over the wireless network; and

3.2.2.2. The design, development, testing and deployment of the mobile data applications.

3.3. Managed BlackBerry Service

3.3.1. The BlackBerry mobile email service shall be provided as a fully managed service.

3.3.2. The Service Provider shall manage the BlackBerry Enterprise Server (BES) infrastructure, i.e. the server software and licences.

3.3.3. The BES infrastructure shall have no single point of failure.

3.3.4. The Service Provider shall load-balance users across the resilient BES infrastructure. “Priority 1” users shall be distributed across the available servers.

3.3.5. The Service Provider shall provide TfL with the BlackBerry asset management information for connected devices, software licences, etc. in order to enable TfL to populate their Configuration Management Database (CMDB).

3.4. Mobile Service Desk located at TfL’s premises

3.4.1. The mobile service desk shall be located at a TfL site to be confirmed. TfL will provide suitable accommodation for the Service Desk.

3.5. Project Work and Consultancy

The charges for Project Work or Technical Consultancy relating to Mobile Service are as set out in Schedule 6 or as otherwise provided by advance written notice to TfL by the Service Provider in accordance with the scope of the work required.

SCHEDULE 6 – CHARGES

1 COMMITMENTS

The Charges set out in this Agreement are subject to the following commitments.

Minimum Term	48
Minimum Period	24

a) Minimum Period – New Connections

Each SIM Card provided as a New Connection must remain connected to the Wireless Services for the Minimum Period commencing on the date it is first connected.

b) Minimum Period – Re-signing Connections

Each SIM Card provided as either a Re-sign SIM-Only Connection or a Re-sign Non SIM-Only Connection must remain connected to the Wireless Services for the Minimum Period which shall commence upon the Commencement Date of this Agreement.

2 AIRTIME CHARGES

2.1 Voice Services

The following are the Airtime Charges relating to tariff(s) available to all parties entering into a Call-Off Contract under the terms of the framework agreement

Airtime Tariff Description	Number of SIM Cards	Invoiced Line Rental Charge	Reduced Line Rental Charge
Mobile Extension 2001	Up to 13,000	£1.50	£1.50
	13,000 – 15,999	£1.50	£1.35
	16,000 – 20,999	£1.50	£1.15
	21,000 – 29,999	£1.50	£0.75
	More than 30,000	£1.50	£0.50

a) The Line Rental Charge set out above applies on a per SIM Card per month basis.

b) The Line Rental Charges shall be invoiced at £1.50 in accordance with the table above. The Service Provider shall review the number of SIM Cards connected to the Mobile Extension 2001 tariff and the BlackBerry from O2 with Mobile Extension 2001 tariff at the end of each monthly invoice period (the "Line Rental Effective Date"). For the purposes of this review, the number of SIM Cards includes applicable SIM Cards under all Call-Off Contracts under this Agreement. If the review demonstrates a new threshold has been reached in accordance with the 'Number of SIM Cards' column in the table above, the Service Provider will calculate the difference between the 'Invoiced Line Rental Charge' and the 'Reduced in Line Rental Charge' from the Line Rental Effective Date (the "Line Rental Credit"). The Service Provider will credit the Call-Off Contract parties' Airtime Account with the Line Rental Credit on an annual basis, or on a six-monthly basis if agreed between the parties. Alternatively, if any Customer connects a significant amount of additional SIM Cards which results in the number of SIM Cards reaching a new threshold, and the parties agree that a change in the actual invoiced Line Rental Charge is more appropriate than issuing Line Rental Credits, then the Service Provider shall carry out the necessary implementation process to change the invoiced Line Rental Charge to the applicable Reduced Line Rental Charge.

c) During the Minimum Term the Customer will be charged for the following call types at the rates shown in the table below:

UK Mobile Originating calls (pence per minute/message)			
	Peak	Off-Peak	Weekend
National Call	2.50	2.50	2.50
Local Call	2.50	2.50	2.50
O2 to O2 calls (On-Net)	0.00	0.00	0.00
O2 to O2 calls	2.50	2.50	2.50
O2 to Other Network Operators	9.00	9.00	9.00
Mobile originating SMS	4.00	4.00	4.00
Voicemail Retrieval	0.00	0.00	2.50
O2 Group Conferencing	3.5p	3.5p	3.5p
UK Land Originating Calls (pence per minute/message)			
	Peak	Off-Peak	Weekend
Land to O2 calls (On-Net)	3.50	3.50	3.50
Land to O2 Calls	5.50	5.50	5.50
Land to Other Network Operators	8.00	8.00	8.00

Charges for all other call types will be charged at the rates set out in the O2 Price List.

d) Calls to Directory Enquiries 118402 are charged at £0.51 pence per minute or part thereof for the duration of the Minimum Term. Calls to all other Directory Enquiries numbers are charged at the rates set out in the O2 Price List.

e) The Airtime tariff set out above includes the International Traveller Service at no extra Line Rental Charge. International call Charges shall be charged in accordance with the table below for the duration of the Minimum Term:

Zones	UK Outbound	Back to UK	In Country	In Zone	Out of Zone	Received Roaming	Text Messages
1	11.91	29.79	29.79	29.79	79.00	15.00	21.00
2	14.46	29.79	29.79	29.79	79.00	15.00	21.00
3	34.04	80.85	80.85	80.85	179.00	51.06	30.00
4	14.46	90.00	90.00	90.00	179.00	38.30	25.00

5	25.53	59.57	59.57	59.57	179.00	42.55	30.00
6	76.59	119.15	119.15	179.00	179.00	84.26	40.00

Zone definitions are available to view at www.o2.co.uk

f) Business Data Sense

The Airtime tariff incorporates Business Data Sense free of any additional Line Rental Charge. Business Data Sense allows you to use the Service Provider's Mobile Web and Mobile Web VPN services and DataLink solutions. The first ½ Megabyte (MB) or 512KB of data usage is free each month, then usage is priced at £1.80 (ex VAT) per MB.

2.2 BlackBerry Services

The following are the Airtime Charges relating to tariff(s) available to the Customer calling off the Blackberry service under this Agreement.

Airtime Tariff Description	Line Rental Charge	Additional Line Rental Charge	Additional Line Rental Charge for Managed BlackBerry Service
BlackBerry from O2	£15.00	N/a	£12.67
BlackBerry from O2 with Mobile Extension 2001 voice service	£15.00	£1.50	£12.67

a) The Line Rental Charge set out above applies on a per SIM Card per month basis.

b) The Airtime tariff set out above includes a call Charge of 10p (ex VAT) for SMS messages sent from the BlackBerry Handheld device. Where a chargeable BlackBerry Voice Service has been selected, SMS messages sent from the BlackBerry Handheld device will be charged at the prevailing rate specified in the chargeable voice tariff. SMS Premium Rate messages will be charged as per the rates set out in the O2 Price List.

c) The Customer may add the Airtime Tariff detailed in section 2.1 of this Charges Schedule as a BlackBerry Voice Service to SIM Cards used in conjunction with BlackBerry Handheld devices subject to payment of the additional Line Rental Charge for Voice as detailed in 2.2 above and any Airtime usage of a SIM Card in conjunction with a BlackBerry Handheld device shall be charged at the voice call rates as set out in that section.

d) The Customer may transfer any SIM Card connected to the Wireless Services under Charges Schedule 2.1 to the BlackBerry Service under this Charges Schedule 2.2 without incurring Termination Charges, subject to that SIM Card remaining connected to the 'BlackBerry from O2 with Mobile Extension 2001 voice service' tariff for a new 24 month Minimum Period commencing on the date of transfer to the BlackBerry Service.

e) The following Charges apply to the BlackBerry e-mail roaming Wireless Service (excluding BlackBerry Voice Service);

Option 1

Monthly Line Rental Charges of £20.00 (ex VAT) per SIM Card which will cover all roaming Blackberry usage for that period. The Line Rental Charges will be charged every month irrespective of whether the Customer roams and is aimed at high roaming users.

Option 2

A daily charge of £5.00 (exc. VAT) per SIM Card per day will cover all roaming usage for that day. The daily charge is only raised if the SIM Card is used while roaming.

a) All SIM Cards will be automatically activated with roaming Option 2 as set out above.

b) BlackBerry Handheld device users may transfer between roaming tariff options 1, and 2 no more than once in any three month period.

c) Software patches (but not upgrades) for the BES Software are included within the Line Rental Charges.

d) Details of the standard call charges associated with the BlackBerry Voice Service can be viewed at: http://www.o2.co.uk/business/tariffs/datatariffs.

2.3 Data and O2 Mobile Broadband Services

The following are the Airtime Charges relating to tariff(s) available to the Customer under this Agreement.

Tariff Description	Number of Xdas ordered	Line Rental Charge	Free of charge Device Included	Inclusive Data	Cost per extra MB	Carry over unused MB
O2 Web Bolt- On	N/A	£6.38	N/A	200 MB	N/A (fair usage policy applies)	No
	1-500	£24.84	Xda Mantle			
		£20.01	Xda Orbit 2			
		£17.26	Xda Atmos			
	500+	£23.99	Xda Mantle			
		£19.40	Xda Orbit 2			
		£17.58	Xda Atmos			
O2 iPhone Bolt- On	N/A	£15.00	N/A	Unlimited	N/A	N/A
Wireless LAN Max	N/A	£12.00	N/A	Unlimited **	N/A	N/A
O2 Mobile Broadband	N/A	£12.77	N/A	3Gb	£0.15	N/A

Additional Conditions for O2 Data Tariffs:

a) The Line Rental Charge set out above applies on a per SIM Card per month basis.

b) Data usage is measured in megabytes (MB). 1MB = 1024 Kilobytes (Kb), 1024 MB = 1 Gigabyte (Gb).

c) Data usage is rounded to the nearest kilobyte on a daily basis and charges are rounded up to the nearest 1p.

d) Each SIM Card is invoiced for the amount of data that travels over the data network. The invoice may include charges for re-sent data packets and packets added to control the flow of data over the network.

e) The Charges set out within this Commercial Schedule do not incorporate data roaming Charges which are set out elsewhere along with a list of the current countries with whom the Service Provider have a roaming agreement.

f) **Fair usage policy of 80 hours per month applies to Wireless LAN Max tariff.

g) The O2 Web Bolt-On tariff, the O2 iPhone Bolt-On tariff and the O2 Mobile Broadband tariffs are allows the Customer unlimited use of O2 UK's GPRS/Edge/3G/HSDPA networks (as applicable to each Device), for internet use via the SIM Card user's handheld mobile device or modem. The Customer agrees that will not user (or permit the use of) SIM Cards:

- In, or connected to, any other device excluding modems; or
- To allow the continuous streaming of any audio/video content, enable Voice over Internet (VoIP), P2P or file sharing; or
- In such a way that adversely impacts the service to other Service Provider customers, including using an excessive volume of data as compared to the majority of users of O2 Bolt On Tariff which is currently more than 200Mb of usage within a one month bill cycle.

h) The current maximum speed available on the O2 Mobile Broadband service on the Service Provider's UK network is 1.36Mbps. However, connection speeds are subject to various factors including network coverage and signal strength and therefore we cannot guarantee that your connection will reach any specific speeds.

i) Text Messages sent from the Connection Manager software will be charged at 10.21p (ex vat).

3 EQUIPMENT CHARGES

A list of Equipment available from time to time from the Service Provider is available upon request. The Service Provider may recommend alternative Equipment where the Customer places an Order for Equipment which has been withdrawn from the range or is temporarily unavailable.

3.1 New Connections

a) Voice Services

Charges for Devices provided by the Service Provider in conjunction with a New Connection are those set out under the Replacement section of the O2 Price List less £35.00 or free of charge whichever is the greater.

b) BlackBerry Services

Charges for Devices provided by the Service Provider in conjunction with a New Connection to the BlackBerry from O2 tariff are those set out under the Replacement section of the O2 Price List.

Charges for Devices provided by the Service Provider in conjunction with a New Connection to the BlackBerry from O2 with Mobile Extension 2001 voice service tariff are those set out under the Replacement section of the O2 Price List less £35.00 or free of charge whichever is the greater.

c) Data Services

Charges for Devices provided by the Service Provider in conjunction with a New Connection to the Data Services set out in 2.3 of this Charges Schedule are those set out under the Replacement section of the O2 Price List.

d) Recovery of Equipment Subsidy

The £35 subsidy in a) and b) above (the "Equipment Subsidy") is based on an expected minimum total expenditure (consisting of Voice, and BlackBerry Line Rental Charges and Airtime Charges only) of £200 per SIM Card during its Minimum Period and in the event that this figure is not achieved the Customer shall repay to the Service Provider an amount equal to the pro-rata value of the Equipment Subsidy.

3.2 Equipment Upgrades/Replacements

Charges for upgrade/replacement Devices provided by the Service Provider are those specified under the Replacement section of the O2 Price List.

3.3 Equipment Accessories

Equipment accessories are available at the Charges set out in the O2 Price List less 15% discount.

3.4 BlackBerry Handheld device Accessories

BlackBerry Handheld device accessories are available at the Charges set out in the O2 Price List.

a) Each BlackBerry Handheld device requires an end-user license in order to use the BlackBerry Service.

b) BlackBerry Handheld devices supplied by the Service Provider are latched to the Service Provider's network. An unlatching code for each device can be supplied at a charge of £10.00 (Ex VAT) per device.

3.5 BES Software

The following Charges apply to the purchase of BES Software;

BES Software including 20 end-user licenses	£2500.00 each
Additional packs of 10 end-user licenses	£350.00 per pack

3.6 Installation Charges with respect to Car Kits

i) Installations will be available at the Charges specified in the O2 Price List.

ii) De - Installations will be available at the Charges specified in the O2 Price List.

iii) De and Re Installations (during the same engineer visit) will be available at the Charges specified in the O2 Price List.

4 PROJECT WORK AND CONSULTANCY

Training - the training rate is £1,500 per day.

Consultancy Services - the rate is £1,500 per day.

Requests for training and consultancy services will be scoped out as and when required.

ADDITIONAL DEFINITIONS

"Airtime"	means wireless airtime and network capacity.
“Airtime Account”	means a notional account set up by the Service Provider to accrue credits owing to the Customer from which Airtime can be purchased from the Service Provider by the Customer.
“BES Software”	means the software known as the BlackBerry Enterprise Server Software and which, when installed on the Customer’s Server of the required Server Specification, forms part of the End-User Licensed Software for the purposes of using the BlackBerry Service.
“BlackBerry Customer Service Charter”	means the service plan for BlackBerry as determined by the Service Provider, which can be provided to the Customer by the Service Provider on request and as updated from time to time.
“BlackBerry Handheld”	means a specific Device the principle purpose of the design of which is for use with the BlackBerry Service or any other Device on which the BlackBerry software is installed for the purpose of using the BlackBerry Service.
“ BlackBerry Internet Solution”	mean the use of the BlackBerry Service in conjunction with compatible Internet based e-mail accounts.
“BlackBerry Service”	means the Wireless Service which enables the Customer to send and receive e-mails using a BlackBerry Handheld and in addition to use the BlackBerry Voice Service and / or the BlackBerry Internet Solution.
“BlackBerry Voice Service”	means the service which enables voice calls to be made and / or received on their BlackBerry Handheld.
“Customer”	means the respective customer (either TfL or any GLA Body) entering into a Call-Off Contract under this Framework Agreement.
"End-User Licensed Software"	means any software, the licence terms for which are governed by a separate agreement with the licensor of such software typically by means of a “click-wrap” or “shrink-wrap” licence agreement.
“First Line Support”	means the Customer’s IT helpdesk which shall be the Customer’s employees’ first point of contact in the event that they have a query or problem with a BlackBerry Handheld or the BlackBerry Service.
"Line Rental Charge"	means the non-usage dependent part of the Charges, payable on a monthly basis per SIM Card.
“Managed BlackBerry Service”	the service whereby the Service Provider provides support to the Customer’s BlackBerry Handheld device as set out in more detail in the Managed BlackBerry Service Charter , and shall form a part of the Wireless Services.
"Minimum Period"	means the minimum number of months each SIM Card provided under this

	Agreement must remain connected to the Wireless Service, which unless agreed otherwise in writing shall be 24 months.
"Minimum Term"	means the term of 48 months from the Commencement Date.
"Mobile Extension"	means the service which uses certain wireless extension technology in conjunction with a private circuit or virtual private circuit and that enables certain Devices to operate as part of the Customer's wireless private or virtual private voice network.
"Network Operator"	means the network operator who operates the wireless network or networks to which the SIM Cards are connected.
"New Connection"	means a new SIM Card (including new SIM-Only Connections and new Non SIM-Only Connections) which connects to the Service Provider's Network under this Agreement which was not immediately prior to this Agreement connected to the Service Provider's Network except where the SIM Cards were formerly provided to the Customer by means of a Reseller;
"Numbers"	means the numbers allocated to the Service Provider by the Network Operator and in turn allocated by the Service Provider to SIM Cards.
"O2 Price List"	means the notes, descriptions and definitions of, criteria for use of, and the list of prices and tariffs which are charged to customers for, Equipment, Wireless Services and the Value Added Wireless Services, and which is supplementary to the Charges Schedule and forms part of this Agreement. The O2 Price List is available at [http://www.o2.co.uk].
"Reseller"	means any third party acting as an agent or distributor on behalf of the Service Provider;
"Re-sign SIM-Only Credit"	means the Credit to be applied to the Equipment Account and/or Airtime Account by the Service Provider in respect of a SIM-Only Re-sign Connection;
"Server"	means the computer server provided by the Customer on which the BES Software will be installed and operate.
"Server Specification"	means the minimum specification of the Server which shall be available from the Service Provider upon request.
"SIM Card"	means the subscriber identity module supplied by the Network Operator (and which shall at all times remain the property of the Network Operator), which is allocated to the Customer by the Service Provider, and which contains the Number.
"SMS"	means the short message service, which enables text messages to be sent to, and received from Devices.

"Value Added Wireless Services"	means the value added Wireless Services such as, installation, insurance, repair etc. as may be made available from time to time by the Service Provider to Business Customers and details of which appear on the O2 Price List.

Additional Terms and Conditions Applicable To The Blackberry Service

The following terms and conditions apply to the BlackBerry Service under the 'BlackBerry from O2' and 'BlackBerry from O2 with Mobile Extension 2001 voice service' tariffs. If the Customer chooses to connect to the Managed BlackBerry Service then the terms and conditions as set out in the Call-Off Contract for the Managed BlackBerry Service shall apply and the terms and conditions below shall not be applicable.

1.1 Notwithstanding clause 2.1 of the Service Provider's Terms and Conditions for Business Customers, where the Service Provider supplies to the Customer Equipment comprising of a BlackBerry Handheld manufactured by Research In Motion, then notwithstanding delivery and acceptance of such Equipment, title in such Equipment will not pass to the Customer until the date on which all invoices relating to such Equipment have been paid in full to the Service Provider.

1.2 The customer expressly acknowledges the following additional obligations in respect to the provisions of the BlackBerry Service;

1.2.1 The Customer shall be responsible for

a) procuring and commissioning the Server in accordance with the Server Specifications; and
b) installing the BES Software; and
c) provision of suitably qualified IT personnel who have a full working knowledge of the Customer's corporate e-mail system and firewalls; and
d) configuration of the BES Software for each BlackBerry Handheld device; and
e) ensuring that any of its staff who will provide First Line Support have received the training which the Service Provider will provide in accordance with this Agreement; and
f) provision of First Line Support for BlackBerry Handheld device users; and
g) provision of any necessary training for BlackBerry Handheld device users; and
h) integration of the Customer's email accounts with the BlackBerry Internet Solution, including but not limited to resolving any issues arising from the interface with the Customer's email internet service provider and/or Customer's IT infrastructure and policy.

1.2.2 The Customer recognises that if it uses software packages or applications other than those approved by the Service Provider for use with a BlackBerry Handheld device or the Server, the Service Provider shall have no liability whatsoever for any failure of the BlackBerry Service resulting from the use of such software packages or applications by the Customer.

1.2.3 The Customer agrees that it will deactivate any lost, stolen or replaced BlackBerry Handheld devices from the Server.

1.2.4 The Customer shall use the returns process as detailed by the Service Provider to the Customer from time to time for returns of all damaged/faulty BlackBerry Handheld devices and/or other Equipment.

1.2.5 The Customer will take all reasonable steps to ensure that all its BlackBerry Handheld device users invoke password protection on their BlackBerry Handheld devices. The Service Provider shall not be liable for any losses whatsoever or howsoever occurring as a result of a BlackBerry Handheld device user failing to invoke adequate password protection. The Customer should note, and inform its users, that text messages as well as emails are retained on a BlackBerry Handheld device even when it is turned off or the SIM Card is removed from it.

1.2.6 The Customer undertakes to comply with all statutory requirements in relation to the use of the BlackBerry Handheld devices and/or other Equipment and the Wireless Services. The Customer shall be responsible, as licensee of the End-User Licensed Software for any encryption of information between the Customer's BES Software and the BlackBerry Handheld devices. The Customer shall accept responsibility for the provision, when properly required, of unencrypted information to the relevant authorities in accordance with European regulations and United Kingdom legislation. In the event that changes in legislation impose a requirement on the Service Provider to provide such unencrypted information, the Customer shall provide the Service Provider, promptly or in accordance with any statutory timescales, with the unencrypted information in order for the Service Provider to forward it to the relevant authority.

1.2.7 the Service Provider reserves the right to upgrade and change the specification of the BlackBerry Internet Solution at any time. This may entail, but is not limited to, changes to the web interface, rules around the maximum number of days that data will be retained and mailbox capacity.

SCHEDULE 7 - DELIVERY REQUEST FORM AND CALL OFF CONTRACT

Transport for London
London Underground Limited

Delivery request

Vendor address

Page 1 of 1

Contact

Requested by :

Telephone :

Invoice to

London Underground Limited
Accounts Payable
4th Floor, West Wing,
55 Broadway
London
SW1H 0BD

Delivery address

London Underground Limited
55 Broadway
London
SW1H 0BD
Or as agreed below

Information

Delivery request no. :
Date :
Vendor no. :
Currency :
Payment terms :

Proposal ref no. :
Contract/P.O number :

Instructions to vendor
The supply of goods/services under this delivery request is subject to the terms and conditions of the contract/purchase order referenced above.

Item	Description	Quantity	UM	Net price	Total price
	Sub Totals				
	Total Cost (excl. VAT)				

Procurement Department:
VAT number 756 2770 08

Date:

MAYOR OF LONDON If you have problems reading this text please call 0207 2225600

GREATER LONDON AUTHORITY

Delivery Request

Vendor address

Contact:

Requested by:

Telephone:

Contract No/PO:

1.1.1 Invoice to
Greater London Authority
PO Box 44425
London
SE1 2UT

1.1.2 Delivery address
Greater London Authority
Technology Group
LGF, City Hall
The Queen's Walk
More London
SE1 2AA

Instructions to vendor

The supply of goods/services under this delivery request is subject to the terms and conditions of the contract/purchase order referenced above.

Item	Description	Quanity UM	Net Price	Total Price
	Sub totals **Total costs (excl. VAT)**			

VAT Number [ ] **Date:**

MAYOR OF LONDON **If you have any problems reading this text please call [ ]**

Example of Implementation of Call Off

Call- Off Contract — T*f*L

THIS CALL- OFF CONTRACT is made on this day of (**"Effective Date"**).

BETWEEN

(1) **TRANSPORT *FOR* LONDON**, a statutory corporation whose principal office is at Windsor House, 42-50 Victoria Street, London SW1H 0TL ("**T*f*L**") contracting for itself and on behalf of each TfL Group Member;

and

(2) **Telefónica O2 UK Limited**, whose registered address is 260 Bath Road, Slough, Berkshire, SL1 4DX (the "**Service Provider**")

RECITALS

(A) T*f*L and the Service Provider have entered into an agreement of even date which sets out the framework for the Service Provider to provide certain Services to T*f*L (the **"Framework Agreement"**).

(B) This Call-Off Contract sets out the terms upon which the Service Provider shall supply the Services to T*f*L.

(C) T*f*L wishes the Service Provider to provide the specific services described herein pursuant to the terms of the Framework Agreement and the Service Provider is willing to supply the same on the terms and conditions set out herein.

IT IS AGREED as follows:

In consideration of, amongst other things, the mutual promises and covenants set out herein, the Parties agree as follows:

1. Call-Off Contract Contents

1.1 The Framework Agreement shall be incorporated into this Call-Off Contract.

1.2 In this Call-Off Contract the words and expressions defined in the Framework Agreement shall, except where the context requires otherwise, have the meanings given in the Framework Agreement.

2. Services

Specification

2.1 The Functional Requirements for the Services to be performed by the Service Provider pursuant to this Call-Off Contract are set out in to Schedule 3 Products and Services of the Framework Contract.

Timing

2.2 The timetable for any Products or Services to be provided or made available by the Service Provider and the corresponding Milestone Dates are set out in this Call-Off Contract. Each Party shall commence their specific obligations in respect of this Call-Off Contract in accordance with the timing in the Project Plan.

Service Credits

2.3 In the event that the Service Provider fails to meet agreed Service Levels, the provisions of Clause 6.6 (Service Credits) of the Framework Agreement shall apply.

Quality and Best Value

2.4 The management practices that the Service Provider have in place to assure the quality of the goods and services represent are set out in clause 17 (Quality and Best value) of the Framework Contract

3. Call-Off Contract Term

The Call-Off Contract shall continue until the Services have been performed or unless otherwise terminated in accordance with the Framework Agreement, or a term agreed by both parties.

4. Payment

Clause 7 (payment procedures and approvals) specifies the charges payable in respect of this call off and the payment methodology) for each element of the services to be provided under this Call-Off Contract. Charges shall be paid only in accordance with the Framework Agreement**.**

5. Key Personnel and Contract Managers

The Key Personnel in respect of this Call Off and both Parties' Procurement Managers shall be as follows:

(a) Key Personnel

For O2:

Mark Crossley – Account Director

Vickie Noble – Service Relationship Manager

(b) Procurement Managers

For TfL: Chris Rawson – Vendor Manager

For the Service Provider*:* Mark Crossley – Account Director

6. Interfaces

The key interfaces to be developed to support the goods and service that are provided which are set out in Schedule 5 The Supply of the Products / Services of the Framework Contract.

7. Documentation

The documentation to be produced for the Call-Off Contract must comply with the relevant standards from the ISO9000 family of documentation.

8. Change Management

The key principles on which the Service Provider proposes approach to change are based on the principals set out in Schedule 5 Service Management Requirements.

9. Amendments

The Parties agree that the details set out in the Schedules to this Call-Off Contract may be subject to further change and/or clarification, or as may be amended by the parties from time to time by way of an AVC in accordance with clause 33 of the Framework Agreement.

10. Law

This Call-Off Contract shall be construed in accordance with and governed by the Laws of England and Wales and each Party agrees to the exclusive jurisdiction of the English courts.

This Call-Off Contract has been signed by duly authorised representatives of each of the Parties on the date specified above.

SIGNED
For and on behalf of Transport *for* London

Signature: .....

Name: .....

Title: .....

Date: .....

SIGNED
For and on behalf of Telefónica O2 UK Limited

Signature: .....

Name: .....

Title: .....

Date: .....

Call- Off Contract — GLA

THIS CALL- OFF CONTRACT is made on this day of (**"Effective Date"**).

BETWEEN

(1) [*Name of GLA Body*], a statutory corporation whose principal office is at [*address*] ("**GLA Body**");

and

(2) **Telefónica O2 UK Limited**, whose registered address is 260 Bath Road, Slough, Berkshire, SL1 4DX (the "**Service Provider**")

RECITALS

(A) Transport for London ("**T*f*L**") and the Service Provider have entered into an agreement of even date which sets out the framework for the Service Provider to provide certain Services to T*f*L (the **"Framework Agreement"**).

(B) T*f*L and the Service Provider have agreed to extend the benefit of the commercial arrangements set out in the Framework Agreement to the GLA Body.

(C) This Call-Off Contract sets out the terms upon which the Service Provider shall supply the Services to GLA Body.

(D) GLA Body wishes the Service Provider to provide the specific services described herein pursuant to the terms and conditions as set out in the Framework Agreement and the Service Provider is willing to supply the same on the terms and conditions set out herein.

IT IS AGREED as follows:

In consideration of, amongst other things, the mutual promises and covenants set out herein, the Parties agree as follows:

1. Call-Off Contract Contents

1.1 The terms and conditions of the Framework Agreement shall be incorporated into this Call-Off Contract.

1.2 In this Call-Off Contract the words and expressions defined in the Framework Agreement shall, except where the context requires otherwise, have the meanings given in the Framework Agreement and for the purposes of this Call-Off Contract the GLA Body will assume the rights and obligations as ascribed to TfL in the Framework Agreement.

1.3 The specified limits of liability set out in clauses 20.1 and 20.5 of the Framework Agreement are hereby varied for the purposes of this Call-Off Contract and shall be set at 100% of the value of the Services provided or to be provided by the Service Provider under this Call-Off Contract to the GLA Body in the relevant Year, or to such other limit as agreed in writing by the parties to this Call-Off Contract.

1.4 The GLA Body and the Service Provider agree and acknowledge that neither TfL nor the TfL Group shall in any way be liable for the GLA Body's obligations arising out of this Call-Off Contract. Notwithstanding anything within the Framework Agreement, no third party shall have any rights under this Call-Off Agreement pursuant to the Contracts (Rights of Third Parties) Act 1999.

2. Services

Specification

2.1 The Functional Requirements for the Services to be performed by the Service Provider pursuant to this Call-Off Contract are set out in to Schedule 3 Products and Services of the Framework Contract.

Timing

2.2 The timetable for any Products or Services to be provided or made available by the Service Provider and the corresponding Milestone Dates are set out in this Call-Off Contract. Each Party shall commence their specific obligations in respect of this Call-Off Contract in accordance with the timing in the Project Plan.

Service Credits

2.3 In the event that the Service Provider fails to meet agreed Service Levels, the provisions of Clause 6.6 (Service Credits) of the Framework Agreement shall apply.

Quality and Best Value

2.4 The management practices that the Service Provider have in place to assure the quality of the goods and services represent are set out in clause 17 (Quality and Best value) of the Framework Contract

3. Call-Off Contract Term

The Call-Off Contract shall continue until the Services have been performed or unless otherwise terminated in accordance with the Framework Agreement, or a term agreed by both parties.

4. Payment

Clause 7 (payment procedures and approvals) specifies the charges payable in respect of this call off and the payment methodology) for each element of the services to be provided under this Call-Off Contract. Charges shall be paid only in accordance with the Framework Agreement.

5. Key Personnel and Contract Managers

The Key Personnel in respect of this Call Off and both Parties' Procurement Managers shall be as follows:

(a) Key Personnel

For O2:

[*name(s) & title (s)*]

(b) Procurement Managers

For GLA Body [*name & title*]

For the Service Provider*:* [*name & title*]

6. Interfaces

The key interfaces to be developed to support the goods and service that are provided which are set out in Schedule 5 The Supply of the Products / Services of the Framework Contract.

7. Documentation

The documentation to be produced for the Call-Off Contract must comply with the relevant standards from the ISO9000 family of documentation.

8. Change Management

The key principles on which the Service Provider proposes approach to change are based on the principals set out in Schedule 5 Service Management Requirements.

9. Amendments

The Parties agree that the details set out in the Schedules to this Call-Off Contract may be subject to further change and/or clarification, or as may be amended by the GLA Body and the Service Provider by agreement in writing.

10. Law

This Call-Off Contract shall be construed in accordance with and governed by the Laws of England and Wales and each Party agrees to the exclusive jurisdiction of the English courts.

This Call-Off Contract has been signed by duly authorised representatives of each of the Parties on the date specified above.

SIGNED
For and on behalf of [*GLA Body*]

Signature: .....

Name: .....

Title: .....

Date: .....

SIGNED
For and on behalf of Telefónica O2 UK Limited

Signature: .....

Name: .....

Title: .....

Date: .....

SCHEDULE 8 - FORM FOR VARIATION

Agreement Parties: [*to be inserted*]

Call-Off Contract Number: [*to be inserted*]

Variation Number: [*to be inserted*]

TfL Contact Telephone [*to be inserted*]

Fax [*to be inserted*]

Date: [*to be inserted*]

AUTHORITY FOR VARIATION TO AGREEMENT (AVC)

Pursuant to Clause 33 of this Agreement, authority is given for the variation to the Services and the Charges as detailed below. The duplicate copy of this form must be signed by or on behalf of the Service Provider and returned to the Call-Off Co-ordinator as an acceptance by the Service Provider of the variation shown below.

DETAILS OF VARIATION	**AMOUNT (£)**
ALLOWANCE TO TFL	
EXTRA COST TO TFL	
TOTAL	

.....
For TfL

ACCEPTANCE BY THE SERVICE PROVIDER	
Date	**Signed**

SCHEDULE 9 – TFL POLICIES AND STANDARDS

Electronic Communications (Including Email and Internet) and Equipment Usage Policy

Issue date: 18 May 2007
Effective: 21 May 2007
Updated: 4 February 2008
This supersedes any previous policies

Index

Electronic Communications (Including Email and Internet) and Equipment Usage Policy

1. Introduction

Transport for London (TfL) aims to provide electronic communications technology and equipment which will enable employees to perform their roles to the highest standards. This will contribute to the operational success of the business and the achievement of its vision and objectives. Electronic mail (email), TfL Intranet (Source) and the Internet are essential business tools which employees must use effectively and appropriately.

2. Organisational Scope

Employees of TfL, Docklands Light Railway Limited, Rail for London Limited, London Bus Services Limited, London Buses Limited, Victoria Coach Station Limited who are on TfL employment contracts (Paybands 1-5 and Directors) and those staff on predecessor organisation employment contracts where the individual has transferred to the employment of TfL.

3. Policy Statement

TfL's main purpose in providing facilities for email, internet and electronic communications is to support its business activities. This policy sets standards so that employees understand how email, Source, the Internet and all other electronic and communications equipment should be used. It complies with current legislation and alerts employees to the need to be aware that breaches of this policy may lead to disciplinary action being taken against them. Where such breaches are deemed to be gross misconduct, disciplinary action may result in dismissal.

4. Requirements

4.1 All information and communications (ICT) equipment, in whatever form, relating to TfL's business activities and all information handled by TfL relating to other organisations with which it deals is subject to this policy.

4.2 TfL's ICT resources include the following: any computer (including laptops issued for off-site use), mobile and handheld devices (e.g. Blackberries, PDAs, XDAs etc), server or network equipment and any telephone handset, switchboard or voice network provided or supported by TfL. It also includes any data stored, processed or transmitted on such networks and data/programs stored on TfL's computer systems or on magnetic or optical storage media that is owned and/or maintained by TfL.

4.3 This extends to an employee's own, or a third parties, computer equipment, when employees are working on the Company's business away from TfL's premises, or using such equipment on its premises.

4.4 TfL reserves the right to monitor and/or record individual use of ICT facilities for legitimate purposes to protect against misuse and to ensure system and operational efficiency and integrity. It reserves the right to access individual accounts in circumstances where it has a reasonable belief that there has been

a breach of this policy.

4.5 Employees should therefore have no expectation of privacy whilst using ICT facilities, including using company equipment for the purposes of communicating via email or in accessing or passing on information obtained through the Internet. Copies of emails may be disclosed to third parties for legal reasons which may include, amongst others, requests made under the Data Protection Act and/or the Freedom of Information Act or in connection with a Court or Tribunal orders for disclosure.

4.6 TfL reserves the right to temporarily or permanently limit, withdraw or restrict the use of, or access to, any ICT facilities if they are used in a way that contravenes this policy.

4.7 Any information created in the course of employment at TfL becomes the property of TfL and may not be used for any other purpose unless approved by the employee's manager. It is the responsibility of employees to ensure that any such work is managed in accordance with TfL's policies and procedures.

4.8 Employees must take all reasonable steps to safeguard the security of ICT systems and the information contained upon them. This includes not allowing unauthorised users access to ICT systems and protecting them from physical damage. They must only access ICT facilities, including email and the Internet via their personal user account and not use or attempt to use another users' account

5. Responsibilities

5.1 All employees:

- must ensure that they do not download, create or transmit material that is abusive or threatening to others or might be regarded as offensive on the basis of personal characteristics such as race, sex, colour, religion, nationality, gender, disability, sexual orientation or age. Where such material is received or stored on personal equipment and brought into the workplace, employees must not show, print, forward or transfer such material on to TfL equipment whilst on TfL premises
- must report it to their manager immediately if any such material is accessed accidentally
- must normally use these facilities for business purposes only
- may use them for limited personal use provided this does not interfere with their work performance and are outside their normal working hours
- must ensure that their usage of TfL's ICT equipment is lawful.
- should contact the IM Helpdesk and their line manager if there is any evidence of misuse

5. 2 All managers and employees with leadership or supervisory roles:

- must take reasonable steps to ensure that the requirements outlined in this policy are adhered to by their employees and that appropriate, fair and consistent action is taken to deal with any failure to conform to them
- should be aware that they can, in some circumstances, be held liable for illegal acts committed by their staff in connection with the use of email or internet or if they fail to maintain adequate supervision

6. Use of Email and Internet

6.1 Email and the Internet are inherently insecure. Confidential, critical or sensitive information should therefore not be sent via email unless there is no reasonable alternative

6.2 Inappropriate or excessive usage could lead to disciplinary action being taken against an employee

6.3 TfL is unable to control the security of personal webmail accounts (such as Hotmail and Yahoo) so these types of account should be avoided for business purposes unless there is no alternative available

6.4 Employees must only use the TfL standard secured connection to the Internet. Unauthorised connections will be considered a serious breach of security. TfL reserves the right to prevent access to certain internet sites

6.5 Employees should not, in normal circumstances share, distribute or amend relevant sections on Source when working with external parties. When seeking to place material on Source, sign off should be obtained from the relevant department head

7. Computer Security

7.1 Employees must:

- keep passwords confidential, not write them down or disclose them to other members of staff, including ICT staff
- ensure that PC/terminals are locked if left unattended. If leaving PC/terminals for a long time or upon leaving the office, employees should ensure that they log off from the system to prevent unauthorised use in their absence. Unless directed otherwise by IM, employees should also close down all electronic equipment at the end of the working day, in line with TfL's initiatives for a sustainable environment

7.2 Employees must not:

- attempt to circumvent any security controls, determine or identify passwords or breach conditional access systems, whether belonging to TfL, its suppliers or third parties
- modify computer equipment provided to employees or input materials onto the system unless authorised to do so
- use or attempt to use ICT facilities or attempt to access data they are not authorised to use or access
- retain TfL information on any non-TfL equipment unless authorised to do so

8. Software

Employees must:

- ensure that software is used legally and in accordance with licensing agreements. Only approved software may be used on TfL computers. If employees are unsure whether software is approved they should refer to their Line Manager or IM
- ensure that all software used on any of TfL's ICT systems is from a reputable and identifiable source, approved in advance by IM Software. Programs,

including unlicensed applications and hacking tools (i.e. programs which provide unauthorised access to other systems) must not be downloaded from the Internet on to TfL ICT systems or sent out via emails

- refrain from infringing third party copyright or licensing requirements when using or copying software for which TfL does not own a current user licence. The making of 'extra' copies of software or the introduction of software packages outside TfL is expressly prohibited
- refrain from using TfL ICT storage provision for personal files, including but not limited to, images, videos and sound files

9. Telephone Usage

9.1 Employees should use TfL telephones (including mobile telephones) for the purposes of TfL business although employees may use telephones to make a reasonable number of personal calls. Use of the telephone system for personal calls is subject to TfL's right to monitor the system for legitimate business purposes. By choosing to use the telephone system to make personal calls you consent to TfL monitoring such calls. TfL reserves the right to claim reimbursement for personal calls made in the event that this privilege is abused. Excessive use of TfL's telephone system for personal use could also have tax implications for employees

9.2 Employees must comply with all relevant legislation in force regarding the use of mobile telephones such as legislation which prohibits the use of mobile telephones whilst operating any vehicle

10. Support and Advice

Support and advice can be obtained through speaking to your manager or contacting HR Services.

11. Ownership and Review

TfL Group Employee Relations and HR Policy

12. Related Documentation

Employees are encouraged to look at this policy in conjunction with:
Code of Conduct
TfL's Employment Framework
Discipline at Work Policy and Procedure
Bullying and Harassment Policy and Procedure
Computer Security and You http://source.tfl/DoingMyJob/Security/3819.aspx
Requirements for the issue and use of Mobile Phones and Pagers
Group IM Information Security Policy

Blocked Files

There are a number of restrictions on the type of files that can be sent by email and downloaded from the Internet. These restrictions are to ensure that the content of files does not compromise the security of TfL through the introduction of viruses, the installation of unauthorised/unlicensed software or copyright theft, for example.

Below is a list of file types that are controlled by TfL IM. This list is based, in part, on government guidelines around the handling of files. Please note that this list will change from time to time to reflect new security threats.

Executable files
These are files that run programs on your computer, e.g. in *Windows* they are recognised by the extension .EXE. Other executable files are recognised by the extensions:

- .EXE, .XPI, .COM, .LNK, .PIF, .SHB, .SYS, .VXD, .HTA, .DLL, .SO, .LIB, .OBJ, .OCX, .VBX, .SCR, .CHM, .SCT, .WSC, .WSF, .WSH, .CPL, .MSC, .REG, .PY, .VBS, .BAT, .CMD, .CSH, .KSH, .SH, .DRV, .MSI

Application files
These are files that are created by applications, e.g. Microsoft Office, and are recognised by the extensions:

- .HLP, .ADE, .ADP, .MDA, .MDB, .MDE, .MDW

Media files
These are files that are used to download music or movies, for example, and are recognised by the extensions:

- .MP2, .MP4, .MP4A, .AAC, .M4A, .M4P, .AC3, .WMA, .WMV, .MPG, .MPEG, .MP3

The sending and receiving of these types of files* by email, either to/from internal colleagues or third parties, and the ability to download these files from the Internet is blocked.

* *Media files may be released if there is a valid business requirement for accessing these files.*

Document Management	
Approved by: Mike Smith Group IM Security Manager	**Date:** June 2006
Custodian: Mike Smith	**Date:** June 2006
Version: V0.1	**Date:** June 2006

Transport for London

GIM STANDARD

Category:	Group Information Management
Number:	IM/TA.01/S01-d2.2
Issue no:	
Issue date:	July 2004

Information Security Standard

Authorised by:		**Date:**	
Approved by:	John Lichnerowicz Head of Group IM Architectures	**Date:**	
Standard owner:	Mike Smith Group IM Security Manager	**Date:**	

Contents

TfL Group Information Security Standard

1 INTRODUCTION & PURPOSE

1.1 All business units (i.e., modes) within the TfL Group need to comply with the TfL Group Information Security Policy. To support this policy, the TfL Group Information Security standard will follow the minimum requirements, structure and referencing of the BS ISO/IEC 17799: 2000 standard (referenced hereafter as ISO 17799), while also meeting the requirements of the government's E-Government initiative and the Turnbull Committee corporate governance initiative.

1.2 The aim of this document is to provide security measures to enable each mode to develop their own Information Security standard, with recommended baseline measures (see Appendix A), using the structure and format of the group standard. Each will incorporate (or cross-reference) the group standard as appropriate in order to ensure that it meets the minimum requirements of the group standard.

1.3 The overall purpose of the group and each mode's versions of the standard will be to provide a security management framework to:

a) protect corporate information **from all threats, whether internal or external, deliberate or accidental**,
b) ensure Information Management (IM) support for business continuity, and
c) minimise business damage by preventing and minimising the impact of security incidents.

1.4 The minimum Information Security requirements for use in contracts with suppliers are given in Appendix B.

2 SCOPE

2.1 Each mode's Information Security standard will apply to the areas of Information Security requirements published as industry best practice in ISO 17799, from which the standard needs to be adapted to reflect the mode's IM environment (with the contents cross-referenced to the specific parts of ISO 17799).

2.2 In addition, the mode's Information Security standard will be expected to support the mode's policies on, for example:

Number	Title	Issue
	Governing safety and security	
	Managing the information systems	

2.3 It is anticipated that the mode's Information Security standard will exclude assessment of risks[1] to individual systems processing the information, which require to be undertaken by relevant System Owners, who will also ensure that their systems satisfy legal and compliance requirements.

3 INFORMATION SECURITY RISK, BASELINE & POLICY REQUIREMENTS

Note on Generic Threats

TfL and each mode require to deal with the following generic threats:

a) Authorised Users and Disaffected Staff

Computer systems are particularly vulnerable to threats from persons who have authorised access to IT systems. They may endeavour, for whatever reason, to obtain information for which they have no "need to know", or even attempt to disrupt the system. Such persons may be casual browsers and persons wishing to sell information on.

[1] Associated with integrity, confidentiality and availability

b) Theft, Loss and Capture

There is ample evidence that IT hardware and components are attractive targets for theft by the criminal community. The small size of modern portable computers, and in particular storage media associated with IT systems, has frequently led to loss.

c) Investigative Journalists

Investigative journalists are increasingly interested in state-run computer systems, particularly those used to support or advise the government. Although there is no evidence of premeditated attempts to acquire information, the information handled by TfL modes would be of interest to them.

d) The Public, Pressure Groups, Anarchists, or Extremist Groups

The fact that information is held electronically and as such is open to novel forms of surreptitious attack presents a special, sometimes intellectual attraction or challenge to individuals who are often known as “hackers”. This threat is enhanced by the growth of computer literacy and applies more specifically to systems that are directly connected to public networks and telephone systems. The information (e.g., personal or operational information) handled by TfL modes would interest them.

e) Accidental Disclosure/Damage by Malicious Software

With the advent of computer systems, information is exchanged quite freely to and from different types of electronic media, e.g., floppy disks, DAT tapes, USB storage and electronic mail. This increases the risks of accidental disclosure of information and damage from malicious software/information imported and exported via magnetic media.

Note on Specific Security Threats & Security Requirements

Specific information security threats that each mode requires to deal with are as follows:

a) Malicious electronic attacks (e.g., denial of service, viruses, manipulation).
b) Physical damage (accidental or malicious) to the building, infrastructure and systems.
c) Insider (accidental or motivated) attack.
d) Outsider (accidental or motivated) attack.
e) Unauthorised introduction of software or hardware by authorised users.
f) Modification of system files by authorised users in order to gain unauthorised access or deny access to authorised users.
g) Unauthorised physical removal of storage media.
h) Mis-configuration of the systems and the networking infrastructure.

To counter the threats identified above, a combination of technical, physical, procedural and personnel measures will need to be employed to protect the mode’s information. Consequently, the following security measures will need to be supported:

i) There will be no anonymous use of the mode’s information systems for the purposes of update/write and delete access.
j) Access to information that is subject to the ‘need to know’ principle will be restricted to authorised personnel who are appropriately cleared and have the need to know.

k) Integrity of information, integrity of the service and availability of information will be maintained.
l) Key hardware that is required to protect information and the network will be physically protected.
m) Update, write and delete operations carried out on the mode's information systems will be attributable to individuals.
n) The mode's information systems will be monitored for breaches in security.
o) There must be effective configuration management.
p) A patching schedule must be agreed and critical patches must be implemented and audited as quickly as possible.
q) All changes must be subjected to a security impact assessment.
r) The security of connections to external systems and networks must be reviewed and only enabled if authorised by the IM Security Manager (or equivalent).

3.1 Based on the high-level baseline summary above of the main security risks and the types of measures that could be taken to counter them, each mode will provide a

a) *Security Statement* (cf. ISO 17799 A 3.1.1), to the effect that it will adopt and promulgate the GIM Information Security Policy;

b) mechanism for the *review and evaluation* (cf. ISO 17799 A 3.1.2) of the Security Statement and the mode's Information Security standard (see section 4.1.1 below).

4 ORGANISATIONAL SECURITY REQUIREMENTS

4.1 Information Security Infrastructure

Control objective: To manage information security within the organisation.

4.1.1 Each mode will set up an *Information Management Security Forum* (IMSF) (cf. ISO 17799 A 4.1.1) to provide direction and management support for security initiatives; to ensure that security aspects of job descriptions are agreed between Information Security and HR; to annually review and evaluate the mode's Information Security standard; and to ensure that information security responsibilities are delegated appropriately.

The Group IM Security Manager will set up a Group Information Security Forum (GIMSF), at which each mode will be represented by the IM Security Manager (or equivalent).

4.1.2 The IMSF will delegate the main responsibility for *Information Security coordination* (cf. ISO 17799 A 4.1.2) to the IM Security Manager (or equivalent).

4.1.3 *Information Security responsibilities* (cf. ISO 17799 A 4.1.3) shall be allocated to (at least) the System Owner, System Operator, IM Solutions Delivery and IM Service Delivery & Support functions.

4.1.4 The IM Security Manager (or equivalent) will *authorise* new security-relevant *information processing facilities* (cf. ISO 17799 A 4.1.4).
System Owners and System Operators should notify the IM Security Manager (or equivalent) about any significant changes affecting security of information. No changes are to be introduced that will or are likely to adversely affect the agreed baseline levels of security of the Group network infrastructure or mode's IM services, without prior authorisation from Group IM Security, or without prior approval and testing.

4.1.5 Group IM Security will provide any *specialist security advice* (cf. ISO 17799 A

4.1.5).

4.1.6 Group IM Security will ensure an appropriate level of *co-operation with organisations* (cf. ISO 17799 A 4.1.6) such as the security, intelligence and enforcement agencies, and maintain contacts regarding potential and actual security incidents.

4.1.7 System Owners and the IM Security Manager (or equivalent) will ensure that the *information security* of systems is subjected to *independent review* (cf. ISO 17799 A 4.1.7) at regular intervals, e.g., 2 years, or annually for critical systems. Such reviews are to be arranged through Group IM Security.

4.2 Security of Third Party Access

Control objective: To maintain the security of organisational information processing facilities and information assets accessed by third parties.

4.2.1 The IMSF and System Owners will be responsible for *identification and assessment of risks to information from third party access* (cf. ISO 17799 A 4.2.1). Group IM Security will require independent reviews of these risks where the systems being accessed are connected to or interface with the group network or systems.

4.2.2 System Owners, together with Procurement, are responsible for ensuring that *security risks* associated with third parties are addressed in the *third party contracts* (cf. ISO 17799 A 4.2.2)

4.3 Outsourcing

Control objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

4.3.1 The IMSF will be expected to ensure that key *security requirements* (e.g., signing of non-disclosure agreements and understanding of IPR) are specified in *contracts with outsourcers or third parties* (cf. ISO 17799 A 4.3.1).

5 ASSET CLASSIFICATION AND CONTROL REQUIREMENTS

5.1 Inventory of Assets

Control objective: To maintain appropriate control of organisational assets.

5.1.1 The Head of Information Management (HIM) or proxy will be responsible for ensuring the creation and maintenance of an *inventory of hardware, software and information assets* (cf. ISO 17799 A 4.5.1), whether in the mode's, third party or employee premises.

5.2 Information Classification

Control objective: To ensure that information assets receive an appropriate level of protection.

5.2.1 Information will be classified in accordance with the mode's *Classification Guidelines* (cf. ISO 17799 A 5.2.1), e.g., TfL Records Management standards (or equivalent).

5.2.2 Information will be *labelled and handled* (cf. ISO 17799 A 5.2.2) in accordance with the mode's document and information management standards, e.g., TfL Records Management standards (or equivalent).

6 PERSONNEL SECURITY REQUIREMENTS

6.1 Security in Job Definition and Resourcing

Control objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

6.1.1 *Job descriptions will include IM security roles and responsibilities* (cf. ISO 17799 A

6.1.1), where appropriate, including either general responsibilities for maintaining compliance with security policy or specific responsibilities for, e.g., protecting particular assets or executing security activities.

6.1.2 Applications for employment shall have *personnel screening* (cf. ISO 17799 A 6.1.2) applied where the job involves access to IT facilities handling sensitive information. Employing managers and HR will be expected jointly to identify 'sensitive' jobs requiring screening, and to define the checks required on the applications (cf. BS 7858: 2004 Security screening of individuals employed in a security environment – Code of practice).

6.1.3 A *confidentiality clause* (cf. ISO 17799 A 6.1.3) will be included in any *contract or agreement* with staff, consultants, contractors or agency staff who will be required to access the mode's information systems. Also, where internal or external resources access systems with sensitive information, they will be given a written statement detailing which systems and particular information they are allowed to access.

6.1.4 In contracts drawn up with staff, business partners or other third parties, the *Terms and Conditions of Employment* (cf. ISO 17799 A 6.1.4) will include a specific clause covering information security.

6.2 User Training

Control objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work.

6.2.1 Employing managers will be expected to ensure that users of IT services receive adequate *education and training for* the systems they are expected to use, *information security* requirements and correct use of IT facilities (cf. ISO 17799 A 6.2.1), as appropriate to their role, before access to IT services is granted.

6.3 Responding to Information Security Incidents and Malfunctions

Control objective: To minimise the damage from information security incidents and malfunctions, and to monitor and learn from such incidents.

6.3.1 Employing managers will ensure that users of IT services are aware of the mode's formal procedure (established with their System Operator) for *reporting information security incidents* (cf. ISO 17799 A 6.3.1) as quickly as possible to the System Owner and the IM Security Manager (or equivalent).

6.3.2 Employing managers will be expected to ensure that users *report information security weaknesses* (cf. ISO 17799 A 6.3.2) to the System Owner and the IM Security Manager (or equivalent). However, information security breaches or concerted attempts by third parties to identify security weaknesses should be reported initially to the IM Security Manager (or equivalent), who would agree an action plan to stop reoccurrence.

6.3.3 Employing managers will ensure that users *report* actual or suspected *software malfunctions*, i.e., any software that appears not to be functioning correctly, to the IT Help Desk (cf. ISO 17799 A 6.3.3) for appropriate action (see Appendix A).

6.3.4 Information security incidents will be reviewed at regular security meetings held by the IM Security Manager (or equivalent) with each System Operator to *learn from the incidents* (cf. ISO 17799 A 6.3.4) and, if required, appropriate action initiated (see Appendix A).

6.3.5 All security incidents will be reported to the Group IM Security Forum by the nominated representatives of the IMSFs.

6.3.6 Any deliberate breach of the mode's security standards and procedures will be treated as a disciplinary matter, and handled in accordance with that mode's *disciplinary procedure* (cf. ISO 17799 A 6.3.5).

7 PHYSICAL AND ENVIRONMENTAL SECURITY REQUIREMENTS

7.1 Secure Areas

Control objective: To prevent unauthorised physical access, damage and interference to business premises and information.

7.1.1 *Physical Security Perimeter* (cf. ISO 17799 A 7.1.1) requirements are that the server for each IT system is located in areas of non-public access to prevent unauthorised access, damage and adverse interference to the mode's information systems, unless the system is specifically designed for public use and is logically isolated from the TfL network. Systems providing access to classified information will be housed in 'sensitive' zones, with appropriately enhanced physical security. The highest level of physical security will be for Secure Zones, typically housing data centres, computer/server rooms and IM communications rooms. The identification of sensitive and secure zones is the responsibility of the IM Security Manager (or equivalent), whilst the specification of the security measures to be applied to these areas will be reviewed and agreed with Group IM Security.

7.1.2 The security of most main office premises is the responsibility of the TfL Property & Facilities Manager, who will determine the actual level of protection required from *physical entry controls* (cf. ISO 17799 A 7.1.2). Business managers will report any concerns about local security arrangements at their offices to the TfL Property & Facilities Manager.

7.1.3 Where possible, all goods will be received within *isolated delivery and loading areas* (cf. ISO 17799 A 7.1.3, and see details in Appendix A).

7.2 Equipment Security

Control objective: To prevent loss, damage or compromise of assets and interruption to business activities.

7.2.1 Where possible, *IT equipment will be sited or protected* (cf. ISO 17799 A 7.2.1) to reduce the risks from theft, environmental hazards, opportunities for unauthorised access and from natural or identifiable man-made disasters, including fire, flooding, dust and loss or fluctuations in the power supply.

7.2.2 *Power supply* equipment (cf. ISO 17799 A 7.2.2) should be installed according to relevant regulations.

7.2.3 Power and telecommunication cabling will be protected from interception or damage by applying *cabling security* measures (cf. ISO 17799 A 7.2.3) to reduce the risks (see examples in Appendix A).

7.2.4 *IT equipment is to be maintained* correctly (cf. ISO 17799 A 7.2.4) to ensure its continued availability, and a record kept of all faults or suspected faults.

7.2.5 Security procedures and controls will cover the *security of IT equipment off-premises* (cf. ISO 17799 A 7.2.5). Each item used outside the mode's premises to support its business activities, regardless of whether it is owned by the mode, a supplier or a contractor, should receive an equivalent degree of security protection as for office equipment (see Appendix A for details). Any equipment taken offsite, which can either directly or indirectly support the mode's information systems, should be treated as if it contains RESTRICTED information.

7.2.6 Company data will be erased prior to the *secure disposal or re-use of equipment* (cf. ISO 17799 A 7.2.6) to avoid it being compromised through lack of care (see

Appendix A for details).

7.2.7 *Company IT assets* (equipment, information, data or software) must not be *moved off-site or to another company site* (cf. ISO 17799 A 7.2.7), without formal authorisation from the relevant System Manager or System / Information Owner, as appropriate, in line with the GIM Asset Management Policy.

8 COMMUNICATIONS AND OPERATIONS MANAGEMENT REQUIREMENTS

8.1 Operational Procedures and Responsibilities

Control objective: To ensure the correct and secure operation of information processing facilities.

8.1.1 System Operators are required to have *documented procedures for correct, secure operation of all IM systems and facilities* (cf. ISO 17799 A 8.1.1), and also for the system development, maintenance and testing, especially if the support of other organisational functions is needed, whether provided by a System Operator or the HIM. Operating procedures will be treated as formal documents, with changes, when necessary, approved through the System Operators' formal change control procedures. In addition, where the change may affect the security architecture, the change will be approved by the IM Security Manager (or equivalent), or where the change is likely to impact Group networks or systems, approval from Group IM will be required

8.1.2 For all services involved in the operation of systems that process company information, System Owners will ensure an appropriate level of configuration management to *control operational change* (cf. ISO 17799 A 8.1.2). Any security related changes (i.e., those affecting the confidentiality, including the protective marking level, integrity or availability of the system) will be referred in advance to the System Owner and the IM Security Manager (or equivalent). Any security measures that are needed as a result will be implemented before the changes are put in place.

8.1.3 An *information security incident management procedure* (cf. ISO 17799 A 8.1.3) is to be implemented to ensure a quick, effective and orderly response to the reporting of such incidents (see Appendix A for details).

8.1.4 System Owners will be responsible for ensuring the *segregation of duties* (cf. ISO 17799 A 8.1.4) in the management and operation of the business unit's information systems. This is required for specific systems processing financial or business sensitive information, or particularly where the processing includes the authorisation of purchases and financial transactions, or as separately required by company Standing Orders, policies or standards.

8.1.5 *Development systems and testing facilities* will be kept securely *separated from operational systems* (cf. ISO 17799 A 8.1.5).

8.1.6 System Owners, in conjunction with the IM Security Manager (or equivalent) and Procurement, will be responsible for ensuring that risks concerned with *external facilities management* (cf. ISO 17799 A 8.1.6) are identified and suitable countermeasures incorporated in relevant contracts. In the case of TfL Corporate staff located in a building covered by another mode, the System Owner will need to check that this is covered under that mode's Information Security standard.

8.2 System Planning and Acceptance

Control objective: To minimise the risk of system failure.

8.2.1 Systems Owners, in close liaison with System Operators, will perform *capacity planning* (cf. ISO 17799 A 8.2.1) to ensure that systems and networks processing the mode's information are capable of meeting the demands in a timely and cost effective manner. Future requirements will need to take into account new system requirements, as well as current and projected needs in computer and network use. All capacity requirements must be reported to the mode's IM function.

8.2.2 System Owners will ensure that the requirements and criteria for *system acceptance* (cf. ISO 17799 A 8.2.2), as detailed in their IM Service Delivery & Support process, are met before the system is placed into live support. Any systems which interface with Group networks or systems must be accepted by Group IM before they are placed into live support.

8.3 Protection against Malicious Software

Control objective: To protect the integrity of software and information from damage by malicious software.

8.3.1 System Owners and System Operators will implement stringent virus detection and prevention *control measures against malicious software* (cf. ISO 17799 A 8.3.1), supported by appropriate user awareness procedures (see details in Appendix A).

8.4 Housekeeping

Control objective: To maintain the integrity and availability of information processing and communication services.

8.4.1 Measures will be needed for *Information Backup* (cf. ISO 17799 A 8.4.1) to ensure:

a) all essential business data and software is secured adequately to enable recovery, in the event of a computer disaster, media failure or corruption due to malicious software (see Appendix A);
b) the backup arrangements meet the IM service continuity requirements of the business continuity plan (see section 11).

8.4.2 System Operators will maintain *Operator Logs* (cf. ISO 17799 A 8.4.2), i.e., records relating to backups, restores, system configuration changes etc, to enable audit and verification of any action. These records will include details of tape movements, as and when backup tapes are moved offsite.

8.4.3 System Operators will maintain a *Fault Logging* (helpdesk) process (cf. ISO 17799 A 8.4.3) to record problems experienced by users, and to ensure that all calls are handled in accordance with SLAs maintained by the IM Service Delivery & Support function.

System Owners, in consultation with System Operators, will set clear rules for the handling of reported faults, including reviewing:

a) fault logs on a regular basis to ensure that faults have been satisfactorily resolved;
b) corrective measures to ensure that security controls have not been compromised, and that the action taken is fully authorised.

8.5 Network Management

Control objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

8.5.1 Firewalls will be implemented as *network controls* (cf. ISO 17799 A 8.5.1) at the boundaries to the Group. Access to the Internet, other public networks and third party networks will be controlled via firewalls managed by the mode. VLANs will be implemented internally on the company LANs, where appropriate. Traffic to and from sensitive applications or information systems will be separated using VPNs.

8.6 Media Handling and Security

Control objective: To prevent damage to assets and interruptions to business activities.

8.6.1 System Owners, in consultation with System Operators, will establish clearly documented procedures for the *management of removable computer media* (cf. ISO 17799 A 8.6.1) such as tapes, disks, cassettes, and printed reports (see Appendix A for details). Removable media will be handled in accordance with their Information Classification label.

8.6.2 System Owners and System Operators will establish clear rules for the secure *disposal of computer media* (cf. ISO 17799 A 8.6.2), to minimise the risk of disclosure (see Appendix A for details).

8.6.3 *Information handling procedures* (cf. ISO 17799 A 8.6.3) will need to be in place to handle sensitive data that requires protection from unauthorised disclosure or misuse. These will cover all sensitive input/output media such as documents, telexes, tapes, disks, reports and any other sensitive items such as blank cheques, invoices etc. System Owners are responsible for ensuring that the areas covered in the procedures will include:

a) handling and labelling of input/output media;
b) maintenance of a formal record of the authorised recipients of data;
c) completion of input data;
d) confirmation of receipt of transmitted media;
e) clear marking of all copies of data for attention of the authorised recipients;
f) review of distribution lists and lists of authorised recipients at regular intervals.

8.6.4 System Owners will ensure that System Operators take all necessary steps for the *security of system documentation* (cf. ISO 17799 A 8.6.4) as protection from unauthorised access, since the documents may contain a range of sensitive information, e.g., descriptions of application processes, procedures, data structures, authorisation processes etc. The measures to be applied include:

a) System documentation must be physically locked in secure cabinets.
b) Distribution of system documentation, firewall rules and network DHCP addresses will be kept to a minimum and controlled. Any systems documentation that needs to be published will be sanitised prior to publication to remove all sensitive information.
c) Computer generated documentation will be stored separately from other application files, and assigned an appropriate level of access protection.

8.7 Exchanges of Information and Software

Control objective: To prevent loss, modification or misuse of information exchanged between organisations.

8.7.1 Formal *information and software exchange agreements* (cf. ISO 17799 A 8.7.1) will be established between the mode and any organisation with which it wishes to have regular interchange of data (e.g., E-commerce transactions with an approved supplier), before initiating the exchange of data and software (electronic and manual). The agreements will specify appropriate security conditions, including:

a) Management responsibilities and procedures for controlling and notifying transmission, despatch and receipt within each participating organisation.
b) Procedures for notifying transmission, despatch and receipt.
c) Minimum technical standards for packaging (to protect the contents from any physical damage) and transmission.
d) Courier identification standards.
e) Responsibilities and liabilities in the event of loss of data.
f) Data and software ownership and responsibilities for data protection, software copyright compliance and similar considerations.

g) Technical standards for recording and reading data and software.
h) Any special measures required to protect very sensitive items, such as encryption keys.

Sensitive information transmitted electronically is to be in encrypted form, with appropriate authentication mechanisms to positively verify the identity of both parties.

8.7.2 As computer media can be vulnerable to unauthorised access, misuse or corruption during transportation, the following measures will be applied to safeguard the *security of computer media in transit* (cf. ISO 17799 A 8.7.2) between sites:

a) Reliable transport or couriers will be used, and a procedure established to check the identification of couriers.
b) Packaging must be sufficient to protect contents from any physical damage likely to happen during transit, with special protection given to classified information through use of locked containers, hand delivery, tamper-proof packaging or, in exceptional cases, splitting the item into more than one delivery and sending the parts by different routes.

8.7.3 System Owners and System Operators will agree with the mode's trading partners (i.e., suppliers approved by Group Procurement) the *electronic commerce security* (cf. ISO 17799 A 8.7.3) controls to be applied to E-commerce transactions. The nature of the controls, which are to be approved by the IM Security Manager (or equivalent), will depend on the information classification and maximum value of the transaction. Where the E-commerce system interfaces with Group networks or systems, then formal approval of the controls will be required from Group IM Security.

8.7.4 As electronic mail (e-mail) has different characteristics from traditional forms of business communications, it requires specific *e-mail security controls* (cf. ISO 17799 A 8.7.4) to reduce business or security risks. While e-mail should not generally be used for anything other than unclassified information, in exceptional circumstances, it may be used to transmit more sensitive information, provided that appropriate security measures are applied. Encryption will be required as a minimum when sensitive information is sent outside the mode's WAN. In addition, information classified as secret needs to be encrypted when sent over the internal e-mail network.

8.7.5 System Owners will be responsible for ensuring that users are provided with suitable procedures for the *security of all electronic office systems* (cf. ISO 17799 A 8.7.5), which will be secured by security hardening, with all unnecessary facilities removed and default passwords changed upon installation.

8.7.6 *Publicly available systems* (cf. ISO 17799 A 8.7.6) will be treated as untrusted, with appropriate measures implemented to protect the internal network and resources. Information would only be released to a publicly available system once this has been authorised by the System Owner. While appropriate security safeguards should be implemented to ensure the integrity and authenticity of communications, by default, there will be no access to publicly available systems without prior approval of the IM Security Manager (or equivalent). The System Operator will control and monitor the integrity of information electronically accessible by the public. The business will manage the firewalls which mediate all communications with public systems.

8.7.7 Concerning the *other forms of information exchange* (cf. ISO 17799 A 8.7.7), telephones are not be used for the discussion of sensitive information. Fax is not be used to send sensitive information, unless the originator has used procedural means to confirm that the recipient is at the receiving fax unit to collect the faxed item. Where information is being transported by other 'offline' means, appropriate

measures are to be taken, in line with 8.7.2 above (see Appendix A for handling of sensitive information sent by Royal Mail).

9 ACCESS CONTROL REQUIREMENTS

9.1 Access Control Business Requirement

Control objective: To control access to information.

9.1.1 In terms of the mode's *access control policy* (cf. ISO 17799 A 9.1.1), System Owners will formulate and maintain a formally documented procedure for requesting, authorising, granting, reviewing and revoking access to computer resources. The procedure will reflect the security requirements of the business application, the corporate and departmental policies for information dissemination and entitlement, and legal obligations to protect access to data (see Appendix A for details of controls).

9.2 User Access Management

Control objective: To ensure that access rights to information systems are appropriately authorised, allocated and maintained.

9.2.1 A formal *user registration and de-registration procedure* (cf. ISO 17799 A 9.2.1) will be established for all access to IM (including desktop) services, ensuring that:

a) The System Owner has authorised the user to use the service, with a level of access appropriate for the business purpose, according to the mode's security policy.
b) If access is granted to information classified as confidential or secret, the user will be given a written statement of his/her access rights, outlining the conditions applicable (including the user having to sign an agreement to comply with the access conditions).
c) Access is only granted when the authorisation procedure is satisfactorily completed.
d) A register of all persons permitted to use the service is established and maintained.
e) All access rights of persons who have left the mode are deleted as soon as advised by the employing manager or, for those who have changed jobs, amended within seven days.
f) All accounts unused for 90 days should be disabled and, if they continue to be unused for a further 90 days, deleted.

9.2.2 In terms of *privilege management* (cf. ISO 17799 A 9.2.2), the granting of special privileges, such as those given to system operators and administrators, is to be kept to the minimum necessary for the proper administration of systems. Privileged accounts are not be used for normal office use, and E-Mail and Internet access not granted, unless with the express permission of the IM Security Manager (or equivalent). In the case of systems with interfaces to Group Networks or Systems, approval will be required from Group IM. System Owners will approve and track the issue of special privileges to users, and review the issue every 6 months.

9.2.3 As part of the System Owner's *management of user passwords* (cf. ISO 17799 A 9.2.3), users with access will be identified uniquely to allow proper management of access controls and to help create comprehensive audit trails for activity carried out on the system (see Appendix A for password management practices).
Unauthorised use of a user-id will be considered a security incident.
In exceptional circumstances, where there is a clear business benefit and subject to agreement by the IM Security Manager (or equivalent) or Group IM (in the case of Group networks or systems), shared user-ids may be used.

9.2.4 System Owners will carry out a formal *review of access rights* (cf. ISO 17799 A 9.2.4) at least once every six months or, for business critical or sensitive systems, at least once every three months. Accounts unused for 90 days will be disabled and, if they continue to be unused for a further 90 days, deleted.

9.3 User Responsibilities

Control objective: To prevent unauthorised user access.

9.3.1 Users will ensure that their *password use* (cf. ISO 17799 A 9.3.1) conforms to security best practice, as defined in 9.2.3 above (and Appendix A), and that each password is:

a) kept confidential (i.e., not written down) and not disclosed to others, except when required to facilitate maintenance, in which case, it must be immediately changed;
b) not reused within eight cycles;
c) changed immediately, if it is thought to be compromised.

9.3.2 When *user equipment (e.g., a terminal) is unattended* (cf. ISO 17799 A 9.3.2) for more than 15 minutes or when the session is finished, users should log-off the service. Where screen savers are used, they should be password protected.

9.4 Network Access Control

Control objective: To protect network services.

9.4.1 The principle on *use of network resources* (cf. ISO 17799 A 9.4.1) is that access to these will be provided on a 'need to use' basis. System Owners and System Operators will be responsible for specifying the resources that need to be used by their systems.

9.4.2 When a system processes information classified as confidential or secret, a routing control mechanism or *enforced path (*cf. ISO 17799 A 9.4.2) will be used to choose routes either dynamically or by some pre-arrangement that uses only physically secure links. Routing controls will be based on positive source and destination address checking mechanisms, which may be implemented in either software or hardware.

9.4.3 Access by remote users will be via strong *user authentication mechanisms for external connections* (cf. ISO 17799 A 9.4.3), namely, a two factor process, i.e., something a user has (an authentication token) and something a user knows. Remote access will be protected by using 'one time' dynamic passwords.

9.4.4 All requests for connection from remote systems on remote networks must be properly authenticated, either by the application system or at the network level, in which case, a *node authentication system* (cf. ISO 17799 A 9.4.4) must be employed to authenticate the remote system (see Appendix A).

9.4.5 Concerning the *remote diagnostic port protection* principle (cf. ISO 17799 A 9.4.5), engineers who need to remotely maintain systems within the mode's environment will use the corporate remote access solution, with appropriate controls (including a strong authentication mechanism) to limit access on these accounts to only those systems that they need to maintain.

9.4.6 Approved VPNs or separate networks should be used to secure access to information classified as Confidential or Secret. The IM Security Manager (or equivalent), in conjunction with the relevant System Owner, should be responsible for determining if *segregation in networks* (cf. ISO 17799 A 9.4.6) is necessary.

9.4.7 Firewalls, VLANs and VPNs are to be used to restrict access on shared networks, in accordance with the access policy on *network connection control* (cf. ISO 17799 A 9.4.7). System Operators will be responsible for ensuring that:

a) all system hardware is inspected on a regular basis for signs of tampering,
b) servers and their direct environments are in a tidy and secure state, and
c) records are kept of the inspection.

Other security measures are covered in Appendix A.

9.4.8 Firewalls, VLANs and VPNs will be used to restrict and *control routing on networks* (cf. ISO 17799 A 9.4.8).

9.4.9 System Operators associated with the LANs and WAN are responsible for ensuring that the mode's network is clearly defined and remains current, with *secure implementation of required network services* and protocols (cf. ISO 17799 A 9.4.9).

9.5 Operating System Access Control

Control objective: To prevent unauthorised computer access.

9.5.1 There will be *automatic identification of a terminal* (cf. ISO 17799 A 9.5.1) by its unique terminal name and dynamic (DHCP) address.

9.5.2 Users of applications requiring authentication or having update, change or delete facilities will *log on, via a set procedure* (cf. ISO 17799 A 9.5.2), onto the operating systems and, where appropriate, the applications, before being granted access to the mode's information. Access should be via a trusted logon path (see 9.1.1 above). Where network resources are being accessed that require no authentication, such as kiosk applications, separate procedures should be agreed at the IMSF (or the GIMSF, in the case of interfaces with Group networks or systems).

9.5.3 System Operators will manage system management accounts, based on a clear need for access that is subject to periodic review. Access controls are to be applied to enforce the principles of least privilege, individual accountability and 'need to know'. All *users will be identified and authenticated* (cf. ISO 17799 A 9.5.3), in accordance with the principles detailed in 9.1.1 above.

9.5.4 In terms of *password management* (cf. ISO 17799 A 9.5.4), passwords are to be implemented to control access to applications and systems, in accordance with the principles detailed in 9.1.1 above.

9.5.5 As computer systems have one or more system utility programs that may be capable of overriding system and application controls, System Operators will ensure that access to and *use of system utilities* (cf. ISO 17799 A 9.5.5) is restricted and tightly controlled (see Appendix A for particular measures to be applied).

9.5.6 Inactive PCs or *terminals will be timed-out* (cf. ISO 17799 A 9.5.7[2]) to prevent access by unauthorised persons. The time-out facility should clear the screen and close access to the application after a defined period of inactivity (15 minutes).

9.5.7 System Owners will be responsible for identifying the need for curbing access, based on *limiting connection time* (cf. ISO 17799 A 9.5.8) for sensitive applications.

9.6 Application Access Control

Control objective: To prevent unauthorised access to information.

9.6.1 As a *restriction of access to information* (cf. ISO 17799 A 9.6.1), strict logical separation of data will be implemented at the server levels, so that:
a) Production and test data is kept separate.
b) Information subject to 'need to know' restrictions is kept separate.

[2] The *duress alarm to safeguard users* requirement (cf. ISO 17799 A 9.5.6) is not currently applicable within TfL.

Users will only have access to applications and at the level of privilege commensurate with their job requirements, which will be achieved by:

c) Providing menus to control access to application system functions.
d) Restricting user knowledge of data or applications system functions which they are not authorised to access.
e) Controlling the capabilities of users (e.g., read, write, delete, execute only) by data set or specific transactions and by their organisational responsibility.
f) Ensuring that outputs from application systems handling sensitive data contain only the data that is relevant to the user of the output.

9.6.2 System Owners will be responsible, where appropriate, for identifying the need for *isolated computing environments for their sensitive information systems* (cf. ISO 17799 A 9.6.2).

9.7 Monitoring System Access and Use

Control objective: To detect unauthorised activities.

9.7.1 The following measures will be implemented for *event logging* (cf. ISO 17799 A 9.7.1) to enable monitoring of systems for deviations from access control policy and to provide evidence of any security incidents.

a) The operating system will produce an audit log, recording the user identifiers, terminal identifiers and time of events, comprising:
   i) log-ins and log-outs;
   ii) failed log-ins;
   iii) failed accesses;
   iv) automatic time-out / log-out events;
   v) changes to user profiles (e.g., creation, deletion or alteration of access rights, privileges or passwords).
b) At the networking level, the record will account for any changes to the configuration of hardware and software, including changes to rule sets and access control lists.
c) Audit / event logs will be retained on the system for at least 3 months and archived for a further 6 months.

The auditing controls will include:

d) Audit alarms will be configured on the operating systems and firewalls, which will highlight potential/suspected breaches in security and raise alert messages on the system management console so that, where necessary, appropriate action can be taken.
e) Audit logs on servers will be reviewed at least once every two weeks.
f) Audit logs on firewalls will be reviewed daily.
g) Where possible, centralised logging will be implemented to enable consistent and coherent searches to take place.

9.7.2 System Operators will be responsible for *monitoring system use* (cf. ISO 17799 A 9.7.2) regularly, and their findings reviewed at the IMSF and GIMSF (see Appendix A for the events to be monitored).

9.7.3 Computer *clocks will be synchronised* (cf. ISO 17799 A 9.7.2) to ensure the accurate recording of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Computer and communication devices that have the capability to operate a real-time clock are to be set to local standard time, with procedures to check and correct time variations including changeover to/from summer time.

9.8 Mobile Computing and Teleworking

Control objective: To ensure information security when using mobile computing and

teleworking facilities.

9.8.1 Since *mobile computing devices* (cf. ISO 17799 A 9.8.1) such as laptops and PDAs are especially vulnerable to theft and compromise, appropriate measures will be put in place to mitigate this risk (see Appendix A for recommended measures).

9.8.2 Concerning *teleworking* (cf. ISO 17799 A 9.8.2), access to the network will be through systems approved by the mode's IM, using two-factor strong authentication approved by Group IM. Access will be in line with any applicable HR Policy / guideline on Work Life Balance and Homeworking.

10 SYSTEM DEVELOPMENT AND MAINTENANCE REQUIREMENTS

10.1 Security Requirements Analysis and Specification of Systems

Control objective: To ensure that security is built into information systems.

10.1.1 For new systems or enhancements to existing systems, System Owners will undertake an *analysis of security requirements at the system requirements specification stage* (cf. ISO 17799 A 10.1.1). While focusing on automated or logical controls to be incorporated in the system, supporting manual controls are also to be considered. These requirements will also apply when evaluating software packages for business applications (see Appendix A for factors to be considered).

In addition to the recommendations arising from the risk analysis, the additional measures described in the subsections below are to be taken in the specified circumstances for each system being developed.

10.2 Security in Application Systems

Control objective: To prevent loss, modification or misuse of user data in application systems.

10.2.1 Where *input data is to be validated* (cf. ISO 17799 A 10.2.1) to guarantee the integrity of the input data, System Owners will ensure that the following measures are implemented.

a) Checks to detect the following errors:
   i) out-of-range values
   ii) invalid characters in data fields
   iii) missing or incomplete data
   iv) exceeding upper and lower data volume limits.
b) Inspection of hard copy input documents for any unauthorised changes to input data.
c) Procedures to ensure that all changes to input documents are authorised.
d) Procedures for responding to validation errors.
e) Agreed definition of responsibilities of all personnel involved in the data input process.

10.2.2 To *control internal processing* (cf. ISO 17799 A 10.2.2), where the mode's information systems are used to process information classified as Confidential or above, the application system will be validated to ensure that the application is not corrupted by processing errors or through deliberate acts. Automated validity checks will be incorporated into such systems to detect corruption.

10.2.3 Where *message authentication* (cf. ISO 17799 A 10.2.3) is required, the application will verify the integrity of the message by a procedure agreed by Group IM (e.g., using checksums or PKI-based measures).

10.2.4 Where *output data is to be validated* (cf. ISO 17799 A 10.2.4) to guarantee the integrity of the output data, the following measures will be implemented:

a) Checks to detect the following errors:
   i) out-of-range values
   ii) invalid characters in data fields
   iii) missing or incomplete data
   iv) exceeding upper and lower data volume limits.
b) Inspection of hard copy input documents for any unauthorised changes to output data.

10.3 Cryptographic Controls

Control objective: To protect the confidentiality, authenticity or integrity of information.

10.3.1 The *principle on use of cryptographic controls* (cf. ISO 17799 A 10.3.1) is that such controls are to be implemented in operating systems on the networks for systems processing information classified as Secret. A risk assessment will identify the need for such controls.

10.3.2 One way *encryption* (cf. ISO 17799 A 10.3.2) will be used for all passwords to be held on magnetic media. System Owners are to consider encrypting data on servers or data transmitted over the network, particularly where the infrastructure is being used by PFI partners or untrusted parties (e.g., the public). A risk assessment will identify the need for encryption. All encryption schemes must be approved by the Group IM Security Manager.

10.3.3 Where *digital signatures* are used (cf. ISO 17799 A 10.3.3), they should use asymmetric cryptography, and provide appropriate levels of assurance that information signed in this way can be attributed to a specific individual, system or process.

10.3.4 Where *non-repudiation services* (cf. ISO 17799 A 10.3.4) are appropriate, for example, email confirmation messages to the use of PKI, the services will be delivered as part of the application. Where PKI is implemented, the System Owner will ensure that the system is managed and operated securely, with appropriate backup and recovery measures.

10.3.5 All security *key management processes* (cf. ISO 17799 A 10.3.5) are to be approved by the Group IM Security Manager.

10.4 Security of System Files

Control objective: To ensure that IM projects and support activities are conducted in a secure manner.

10.4.1 System Operators will strictly *control implementation of operational systems software* (cf. ISO 17799 A 10.4.1) in order to minimise the risk of corruption of application systems, using appropriate controls (see Appendix A for mandatory and recommended controls).

10.4.2 *System test data will be protected and controlled* (cf. ISO 17799 A 10.4.2), as systems and acceptance testing usually requires substantial amounts of test data that is as similar as possible to operational data. The use of live data containing personal information for testing should be avoided. Appropriate controls (see Appendix A) are to be applied to protect operational data used for testing purposes.

10.4.3 In order to avoid potential corruption of computer programs, *control of access to program source libraries* (cf. ISO 17799 A 10.4.3) will be enforced by the operating system, and access limited to specified System Operators authorised as program librarians (see Appendix A for other possible measures).

10.5 Security in Development and Support Processes

Control objective: To maintain the security of application system software and

information.

10.5.1 System Operators will establish formal *change control procedures* (cf. ISO 17799 A 10.5.1) to ensure that:

a) strict control is maintained over the implementation of changes to hardware, firmware, software and data structures in order to avoid the corruption of information systems.
b) support programmers are given access only to those parts of the system that are necessary for their work.

Before authorisation of changes, System Operators will ensure that:

c) Computer software, programs, data files, database tables and hardware that require amendment are identified.
d) Security controls and integrity procedures will not be compromised by the changes.
e) Changes are accepted by the System Owner before implementation.

System Owners will also ensure that:

f) The system documentation set is updated on completion of each change.
g) Version control records are appropriately updated.
h) An audit log of all changes is maintained.

10.5.2 When the need arises periodically for a change or upgrade to the operating system (e.g., for the installation of a new release), System Owners and System Operators will ensure that there is no adverse impact on the agreed baseline levels of security. Following changes, application systems will be *technically reviewed and tested to ensure operating system changes* (cf. ISO 17799 A 10.5.2) have not compromised application control and integrity procedures.

10.5.3 *Restrictions* or constraints *on changes to software packages* (cf. ISO 17799 A 10.5.3) need to be considered (see Appendix A for details).

The original software will always be retained, with changes applied to a clearly identified copy and fully documented so that they can be re-applied, if necessary, to future software upgrades.

10.5.4 All software and hardware should be purchased from reputable supplier sources to guard against *covert channels and trojan code* (cf. ISO 17799 A 10.5.4). Normally, shareware software should not be used. However, in the event that it is required, such code must be tested and inspected to ensure that it is free from covert channels and any trojan code.

10.5.5 Contracts are to be in place for any *outsourced software development* (cf. ISO 17799 A 10.5.5), which will undergo:

a) formal security testing prior to being accepted.
b) formal acceptance by the System Owner in the mode.

11 IM SERVICE CONTINUITY MANAGEMENT REQUIREMENTS

Control objective*:* To provide IM support for measures to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

Note on Business Continuity Management

A business continuity management process will be implemented by TfL to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.

The consequences of disasters, security failures and loss of service will be analysed. Contingency plans will be developed and implemented to ensure that business processes can be restored within the required timescales. Such plans will be maintained and practised to become an integral part of all other management processes.

Business continuity management will include controls to identify and reduce risks, limit the consequences of damaging incidents and ensure the timely resumption of essential operations.

11.1 Within the context of the TfL *Business Continuity Management* plan and procedures referred to in the Note above (cf. BS Guide PAS 56: 2003 & ISO 17799 A 11.1), the control objective of the each mode's IM function will be to ensure IM service continuity support for the Business Continuity measures.

12 COMPLIANCE REQUIREMENTS

12.1 Compliance with Legal Requirements

Control objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

12.1.1 The standard will be expected to *identify minimum statutory, regulatory and contractual requirements* (cf. ISO 17799 A 12.1.1), amendments and statutory orders to the following:

a) The standard itself
b) Companies Act 1985 (including TfL Group companies' Memorandum and Articles of Association)
c) Computer Misuse Act 1990
d) Copyright, Design and Patents Act 1988
e) Data Protection Act 1998 (DPA)
f) E-Commerce Regulations 2003
g) Freedom of Information Act 2000 (FoIA)
h) Greater London Authority Act 1999
i) Health & Safety at Work etc Act 1974 and legislation made thereunder
j) Human Rights Act 1998 (HRA)
k) Limitations Act 1980
l) Local Government Act 1999, particularly the requirement for Best Value Authorities (including TfL) to secure continuous improvement with regard to Economy, Efficiency and Effectiveness. Aligned to this duty are statutory Best Value Performance Indicators (BVPIs), such as BVPI157 which measures the number of electronically enabled interactions with the citizen and other stakeholders, i.e., e-Government (e-Gov), to which there is an associated standard on the e-Government Interoperability Framework (e-GIF)
m) Public Records Act 1958, and Department for Constitutional Affairs (DCA) Code of Practice on Records Management
n) Regulation of Investigatory Powers Act 2000 (RIPA)
o) Telecommunications Regulations 2000
p) TfL Standing Orders
q) Group Finance Manual
r) Group Information Management Policies, with associated standards and procedures
s) TfL Corporate Business Continuity Management plan and procedures
t) and any other items as may be advised, from to time, by the IM Security Manager (or equivalent).

System Owners will be responsible for identifying and documenting the specific statutory, regulatory and contractual requirements of each system.

12.1.2 Procurement, in conjunction with System Owners, will ensure that aspects related to *Intellectual Property Rights (IPR)* (cf. ISO 17799 A 12.1.2) are specified within any contracts placed with third parties, contractors or staff.

12.1.3 The *safeguarding of organisational records* (cf. ISO 17799 A 12.1.3) is covered by:

a) Companies Act 1985
b) Copyright, Design and Patents Act 1988
c) Data Protection Act 1998
d) Public Records Act 1958
e) DCA Code of Practice on Records Management

To meet statutory and organisational requirements, each mode should take the following steps:

i) Guidelines should be issued on the classification, retention, storage, handling and disposal of records and information.
ii) A retention schedule should be produced that identifies essential record types and the period of time for which they should be retained.
iii) An inventory of sources of key information should be maintained.
iv) Appropriate controls should be implemented to protect essential records and information from loss, destruction and falsification.

12.1.4 *Data protection and privacy of personal information* (cf. ISO 17799 A 12.1.4) is covered by:

a) Computer Misuse Act 1990
b) Data Protection Act 1998
c) Freedom of Information Act 2000
d) Human Rights Act 1998

System Owners are responsible for ensuring that, where the DPA applies, they have passed details of their systems to the TfL Information Compliance Team, who will process notification of purpose under the Data Protection Act. System Owners need to respond in a timely manner to requests for information under the DPA and FoIA, which require to be performed within the timescales prescribed in the Act(s).

Access to system audit tools and intrusion detection systems will be controlled to prevent any possible misuse or compromise, particularly in relation to HR systems, in line with the safeguards of the HRA and the requirements of the Computer Misuse Act, DPA and RIPA.

12.1.5 *Prevention of misuse of information processing facilities* (cf. ISO 17799 A 12.1.5) is covered by:

a) Computer Misuse Act 1990
b) Data Protection Act 1998

Login warning disclaimer messages need to be implemented to ensure that users know that the Computer Misuse Act and Data Protection Act apply. Under these Acts, staff also need to be notified that the mode's information systems are only to be used for official purposes. Their use of emails and Internet may be monitored in the event of any security or disciplinary investigation. All such monitoring of staff is to be approved by both the IM Security Manager (or equivalent) and HR, and is to adhere to the current guidelines on staff monitoring.

12.1.6 The IM Security Manager (or equivalent) will with the Group IM Security Manager approve and *regulate implementation of cryptographic controls* (cf. ISO 17799 A 12.1.6).

All private keys shall have passwords. Where no PKI exists, local managers are

responsible for ensuring that private encryption keys are held securely.

For all centrally distributed key pairs and certificates, the IM Security Manager (or equivalent) or proxy will hold the root Certification Authority certificate and keys. Where possible, all encrypted e-mail will be also encrypted to an administrative key, held by the Group IM Security Manager to allow decryption of e-mail in the event of a request by the Police or Security Services. If such a request occurs, the Information Compliance Manager requires to sign it off.

12.1.7 The Computer Misuse Act 1990 and other legislation cover requirements for *collection of evidence* (cf. ISO 17799 A 12.1.7). However, the Data Protection Act 1998 places on legal persons or entities, who are registered to hold personal information, the need to protect such data against unauthorised access or alteration and also against accidental loss or deliberate destruction. If a security breach occurs, TfL or LUL will be legally obliged to show to the Information Commissioner that all "reasonable" steps have been taken to protect the data. Hence, System Owners will ensure that adequate controls are in place for the collection of the audit trails and similar evidence, which will include collection of the following details:

a) Date and time of unauthorised access.
b) Unique ID of the user who initiated the access.
c) Origin of the request for access (e.g., terminal ID).
d) Name of object involved (e.g., file accessed).
e) Complete details of all unauthorised modifications.
f) Complete details of all deliberate destruction (including physical destruction).

12.2 Reviews of Security Policy and Technical Compliance

Control objective: to ensure compliance of systems with organisational security policies and standards.

12.2.1 Business unit managers and the IMSF (or equivalent) will be responsible for ensuring that IM systems *comply with the Group IM Security Policy* (cf. ISO 17799 A 12.2.1) and with this standard. In the event of a non-compliance with the Group standard, a waiver or concession may be sought from the Group IM Security Manager (see section B.3.2).

12.2.2 The IMSF (or equivalent) will ensure that *technical compliance checking* (cf. ISO 17799 A 12.2.2) is undertaken.

12.3 System Audit Considerations

Control objective: to maximise the effectiveness of, and to minimise interference to/from, the system audit process.

12.3.1 System Owners will plan, agree with auditors and *control audits of operational systems* (cf. ISO 17799 A 12.3.1) so that the risk of disruptions to normal business processes may be minimised, as follows:

a) Audit requirements will be agreed with the System Owner of the application.
b) The scope of checks is to be agreed and controlled.
c) The checks will be limited to read-only access to software and data.
d) All other types of access, other than read-only, will only be allowed for isolated copies of system files, which are to be erased on completion of the audit.
e) IT resources for performing the checks will be clearly identified and made available.
f) All requirements for special or additional processing are to be identified and agreed with System Operators.
g) All access will be monitored and logged to produce a reference trail.
h) All procedures, requirements and responsibilities will be documented.

12.3.2 All *system audit tools (software and data files) will be protected* (cf. ISO 17799 A

12.3.2) to prevent any possible misuse or compromise. They should be separated from development and operational systems and not held in tape libraries or user areas, without appropriate levels of additional security.

13 RESPONSIBILITIES

Control objective: To ensure that each party involved in aspects of Information Security understands their key responsibilities

13.1 Information Management

13.1.1 The Head of Information Management (HIM) for the TfL Group or in each mode will ensure that measures are undertaken so that:

a) Information will be **protected against unauthorised access**.
b) **Confidentiality** of information will be assured.[3]
c) **Integrity** of information will be maintained.[4]
d) **Regulatory** and **legislative** requirements will be met.[5]
e) IM service continuity plans to support the **Business Continuity plans** will be produced, maintained and tested.[6]
f) **Information security training** will be available to all staff.
g) **All breaches of information security,** actual or suspected, will be reported to the Group IM Security Manager, and investigated by the **Group IM Security Manager** or the equivalent in each mode.
h) Procedures will be produced to support this statement.
i) Business requirements for availability of information and information systems will be met.
j) System Owners and System Operators are aware of their respective responsibilities to use or operate IM systems in a secure manner, and to adhere to the Group Information Security Standard.

13.2 Information Management Security Forum

13.2.1 The Group Information Management Security Forum (GIMSF) covering all TfL modes has direct responsibility for:

a) maintaining the Group Information Security Policy and providing advice and guidance on its implementation;
b) authorising changes to the Group Information Security Standard;
c) agreeing and authorising any deviations, waivers or concessions on controls identified in this standard;
d) ensuring that information security responsibilities are delegated appropriately.

13.2.2 This Group Information Security Standard will be reviewed annually by the GIMSF, who will recommend any change for approval by the Group HIM, prior to submission of the change for authorisation and issue under the standards change process.

13.3 System Owners

13.3.1 System Owners in each mode are senior managers who hold the budgets for information systems within their assigned area of control, have the authority for the acquisition, creation, maintenance and disposal of such information systems, and the responsibilities defined within this standard.

---

[3] The protection of valuable or sensitive information from unauthorised disclosure or intelligible interruption.

[4] Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.

[5] This applies to record keeping and controls in place; it includes the requirements of legislation such as the Companies Act and the Data Protection Act.

[6] This will ensure that information and vital services are available to users when and where they need them.

13.4 System Operators

13.4.1 System Operators are the information service providers retained by the IM Service Delivery & Support function in each mode to operate systems under the terms of SLAs, and have the responsibilities defined within this standard.

13.5 Information Owners

13.5.1 Information Owners in each mode are System Owners and are senior managers who have the authority for the acquisition, creation, maintenance and disposal of information/data within their assigned area of control.

13.5.2 Where the information/data in a database is shared by two or more systems, a specific Information/System Owner shall be nominated by the HIM to have overall responsibility for the database containing the shared information/data.

13.5.3 Where information/data derived from multiple sources is manipulated and stored in another target database, it shall be owned by the Information/ System Owner of that target database.

13.5.4 Where information/data stored includes personal details to which the Data Protection Act 1998 applies, the Information/System Owner will inform the TfL Information Compliance Team (see sub-section 12.1.4 for details).

13.6 Information Custodians

13.6.1 Information Custodians are the individuals (i.e., staff from Information Management departments or system administrators, including staff from information service providers retained by the IM Service Delivery & Support function in a mode) in physical or logical possession of information assigned from the Information Owners, for whom they are required to provide information and security services.

13.7 Information Users

13.7.1 Information Users comprise all persons within the TfL Group (i.e., employees, temporary staff, contractors, consultants or other third parties) with whom special arrangements, such as confidentiality and non-disclosure agreements, have been made. Every User must be known to and authorised by a System or Information Owner.

14 SUPPORTING INFORMATION

14.1 Background

14.1.1 The TfL Group's information systems are exposed to many risks which range from thefts to viruses to power failure. The effects could at best be an inconvenience and at worst an expensive or life threatening incident. Most incidents can be readily countered by designing in and implementing security controls following an assessment of the risks to the TfL Group's information.

14.1.2 As the rigour of the controls required depends on the risks to the TfL Group's information, this standard identifies the minimum standards expected of systems processing this information.

14.1.3 As previous IT Security standards within the Group were derived from the industry best practice set out in BS 7799: 1995, this standard has been developed from the updated best practice published in ISO 17799: 2000 and BS 7799-2: 2002, tailored to reflect the TfL Group environment.

14.1.4 This standard will be supported by procedures, guidelines and, from time to time, other documents that define how the standard is to be interpreted concerning specific technologies or threats to security.

15 REFERENCES

15.1 References

15.1.1 Statutory documents

Document no.	Title
	Companies Act 1985
	Computer Misuse Act 1990
	Copyright Designs and Patents Act 1988
	Data Protection Act 1998 (DPA)
	E-Commerce Regulations 2003
	Freedom of Information Act 2000 (FoIA)
	Greater London Authority Act 1999
	Health & Safety at Work etc Act 1974 (and related legislation)
	Human Rights Act 1998 (HRA)
	Limitations Act 1980
	Local Government Act 1999
	Public Records Act 1958
	Regulation of Investigatory Powers Act 2000 (RIPA)
	Telecommunications Regulations 2000
	DCA Code of Practice on Records Management

15.1.2 International Standards Organisation & British Standards

Document no.	Title
BS ISO/IEC 17799: 2000	Information Technology – Code of practice for Information Security Management
BS 7799-2: 2002	Information Security Management Systems – Specification with guidance for use
BS 7858: 2004	Security screening of individuals employed in a security environment – Code of practice
PAS 56: 2003	Guide to business continuity management

15.1.3 Other national standards

Document no.	Title
BS 7799: 1995	Information Security - replaced by BS ISO/IEC 17799: 2000 and BS 7799-2: 2002 on Information Security Management

15.1.4 TfL Group documents

Document no.	Title
	Group Finance Manual
	Group Information Security (policy, standard and procedures)
	TfL Standing Orders

	TfL Business Continuity Management (plan and procedures)

15.2 Abbreviations

The following abbreviations are created:

a) within this document;
b) in Jargon Buster on Intranet;
c) from published sources, e.g., dictionaries;
d) Office for Government Commerce (OGC, source of government IM/IT publications, policies and standards).

Abbreviation	Definition	Source
ACL	Access Control List	a
BCP	Business Continuity Plan	a
CCTV	Closed Circuit Television	b
CESG	Communications and Electronic Security Group (UK Government's Information Assurance Department)	d
CHECK	IT Healthcheck	d
CLAS	CESG Listed Advisor Scheme	d
CRAMM	CCTA (now Office for Government Commerce) Risk Analysis Management Method	d
DAT	Digital Audio Tape (used by IM for data backup)	b
DCA	Department for Constitutional Affairs	a
DHCP	Dynamic Host Configuration Protocol	a
DMZ	De-militarised Zone	d
DPA	Data Protection Act	c
E-commerce	Electronic Commerce	d
E-mail	Electronic Mail	d
FIPS	Federal Information Processing Standard	d
FoIA	Freedom of Information Act	a
HIM	Head of Information Management	b
HMG	Her Majesty's Government	c
HR	Human Resources	b
ICMP	Internet Control Message Protocol	c
IM	Information Management	a
IMSF	Information Management Security Forum	a
IP	Internet Protocol	b
IT	Information Technology	b
LAN	Local Area Network	b
LUL	London Underground Limited	b
MAN	Metropolitan Area Network	b
NISCC	National Infrastructure Security Co-ordination Centre	d
PDA	Personal Digital Assistant	b
PFI	Private Finance Initiative	b
PKI	Public Key Infrastructure	c

RIPA	Regulation of Investigatory Powers Act	c
SLA	Service Level Agreement	b
SMB	Server Message Block (communications protocol)	b
TfL	Transport for London	b
UNIRAS	Unified Incident Reporting and Alert Scheme (run by NISCC)	d
USB	Universal Serial Bus	c
VLAN	Virtual Local Area Network	c
VPN	Virtual Private Networking (encryption)	c
WAN	Wide Area Network	b

15.3 Definitions

The following topic specific definitions are created:

a) within this document;
b) in Jargon Buster on Intranet.

Term	Definition	Source
Asymmetric cryptography	Asymmetric cryptography is also called public key cryptography because the encryption key is made public, usually held in a LDAP (Lightweight Directory Access Protocol) directory, while the decryption key is kept private	a
Critical systems	IM systems identified as critical in the mode's business recovery plan	a
De-militarised Zone	Buffer to hold data between a firewall and internal networks	a
Dynamic Host Configuration Protocol	A protocol that provides a means to dynamically allocate IP addresses (via a DHCP server) to desktop computers and other devices on a local/wide area network	a
Information security incident	Reportable incident includes a system failure and the loss of service; an error resulting from incomplete or inaccurate business data; and a breach or attempt to breach security.	a
Metropolitan Area Network	High-speed WAN connecting LUL's major offices and TfL's Windsor House office	b
Mode	A business unit, e.g., LUL, within the TfL Group	a
Non-repudiation service	A security service that provides protective evidence against false denial (by either the originator or the recipient) of involvement in a communication	a
Restricted information	This usually means material marked as 'Restricted' by HMG; it can also include information held about LUL that is critical to the safe operation of the railway or related information systems, and information that is to be available only to key management and staff within a mode or the TfL Group, i.e., not generally	a

Secure Zone	Area where sensitive or restricted material is being handled	a
Sensitive information	Material defined as 'sensitive' in the Data Protection Act 1998 (DPA)	DPA
Standard	A document issued by a national, international, industry or company authority, which defines overall or minimum requirements with which a product or service shall comply	b
System Operator	Service provider retained by IM Service Delivery & Support to operate a system under the terms of an SLA	a
System Owner	Business manager who holds the budget for the system	a

15.4 Document History

Edition	Date	Changes	Author
D1	January 2004	Reflects industry best practice updated from BS 7799: 1995 to BS ISO/IEC 17799: 2000 and BS 7799-2: 2002.	Mike Smith
D1.2	March 2004	Format updated to meet TfL Design standard.	Mike Smith
D1.3	April 2004	Content of sections 11 and 12.1 updated to meet Business Continuity Management and Compliance requirements.	Mike Smith
D1.4	May 2004	Numbering amended by IM Governance and content of sections 9.1.1, 10.4 and 12.1 updated to meet Access Control, Security of System Files and Compliance requirements.	Mike Smith
R1.0	June 2004	Format updated to meet revised TfL Design standard.	Mike Smith
D2.1	July 2004	Revise format, by moving Section A into Appendix B, part of Section B (sub-sections 6-10) into Appendix A; revise content of subsection 13.5.	Mike Smith
D2.2	July 2004	Revise sub-section 9.8.2 on Teleworking	Mike Smith

APPENDIX A: BASELINE INFORMATION SECURITY MEASURES

Section Action Recommended

A.6.3 Responding to Information Security Incidents and Malfunctions

6.3.3 If the malfunction is suspected to be due to malicious software (e.g., a computer virus), the user will note the symptoms and any screen messages, stop using the computer and inform the IT Help Desk immediately. Recovery will be carried out by trained and experienced IT support staff assigned to the fault by the System Operator.

6.3.4 Where it is identified that changes to procedures or new security controls need to be introduced, these will be implemented via the normal change control procedures. Changes which are likely to impact the security of the Group network or systems must be authorised by Group IM Security.

A.7.1 Secure Areas

7.1.3 Where possible, all goods will be received within isolated delivery and loading areas. In general offices, this will normally be a controlled reception area, while data centres will have a designated loading bay.

A.7.2 Equipment Security

7.2.3 Power and telecommunication cabling will be protected from interception or damage by applying cabling security measures, for example:

a) Place cabling underground or in conduits or, for critical systems, in armoured conduits.
b) Equipment racks must be lockable or alarmed, the master keys being held by the keyholders nominated in consultation with the IM Security Manager (or equivalent). In the case of equipment racks housing Group IM assets, the keyholders will be nominated by the Group IM Security Manager.

7.2.4 The following controls must be applied to IT equipment off-premises:

a) Virus prevention controls must be in place.
b) When travelling, equipment (and media) must not be left unattended in public places. Portable computers (laptops, PDAs etc) must be carried as hand-baggage when travelling.
c) Portable computers are vulnerable to theft, loss or unauthorised access when travelling. Depending on the classification of the information held on such equipment, they must be provided with an appropriate level of access protection to prevent unauthorised access to the information.

7.2.6 Company data will be erased prior to the secure disposal or re-use of equipment, as follows. All equipment containing storage media (e.g., fixed hard disks) must be checked to ensure that any sensitive data and licensed software is removed or overwritten prior to disposal. The overwriting process will involve a multi-pass system. A damaged storage device containing very sensitive data may require a risk assessment to determine if the item must be destroyed, repaired or discarded.

A.8.1 Operational Procedures and Responsibilities

8.1.3 The reportable information security incidents include system failures and the loss of service; errors resulting from incomplete or inaccurate business data; and breaches or attempts to breach security. System Operators will also be responsible for reporting security related incidents to the IM Security Manager (or equivalent). All such incidents will be reviewed at the IMSF and the GIMSF.

In addition, System Operators will be responsible for:

a) procedures for recovery;
b) analysis and identification of the cause of the information security incident;

c) planning and implementation of remedies to prevent recurrence;
d) communication with System Owners and others affected by or involved with recovery from the incident;
e) ensuring that emergency actions taken are documented, reported to management and reviewed.

A.8.3 Protection against Malicious Software

8.3.1 Protection against viruses will be based on good security awareness, appropriate access control, regular scanning of disks and measures such as:

a) Anti-virus products will be implemented on servers and workstations promptly and be updated on a regular basis to ensure the integrity of software and data.
b) All parts of the IM service will be monitored for any potential malicious software, which will be identified, isolated, and removed, with each incident being reported to the IM Security Manager (or equivalent) and to the GIMSF.
c) Electronic mail traffic will be scanned for the presence of viruses and malicious code, using a content scanning product that has been approved by Group IM Security.
d) Where appropriate, all software will be virus checked prior to its installation on the mode's information systems.

A.8.4 Housekeeping

8.4.1 For LAN Backup, System Operators will ensure that every file server on the network is fully backed up in accordance with current Service Level Agreements (SLAs). Certain systems (including any mini and mainframe systems) may have special dispensation from the standard backup regime, where backup schedules are specified in SLAs held by the IM Service Delivery & Support function.

A.8.6 Media Handling and Security

8.6.1 The following practices shall be applied for management of removable media:

a) Use of a data storage system that avoids the use of descriptive labels (i.e., the data stored must not be identifiable from its label).
b) If no longer required, all reusable media will be completely erased before removal from the mode's premises.
c) A written authorisation for the removal of all such media will be issued and a record maintained for audit trail purposes.
d) Storage of all media in a safe and secure environment, in conditions that meet the manufacturer's specification.

8.6.2 The following measures will be applied for the secure disposal of computer media:

a) Media containing sensitive information is to be disposed of securely either by incineration or shredding. Magnetic media is to be completely erased by de-gaussing or by low-level formatting (see sub-section 7.2.6).
b) Disposal of sensitive items should be logged to maintain an audit trail.

The overwriting process will involve a multi-pass system, agreed by the IM Security Manager (or equivalent).

A.8.7 Exchanges of Information and Software

8.7.7 If sensitive information is being sent by Royal Mail, the envelope is to be marked 'private', sent directly to the intended recipient by special delivery, and all joins on the envelope resealed with tape.

A.9.1 Access Control Business Requirement

9.1.1 The following access control requirements will be covered:

<u>Logon Requirements</u>

System Owners will ensure that the system provides a secure logon procedure that:

a) requires entry of a user id and valid password (which is not displayed), and displays system or application identifiers only when the logon process is completed successfully.
b) validates logon information only after all data has been input and, if an error condition arises, does not show an unauthorised user which input data items are correct/incorrect.
c) permits only five unsuccessful logon attempts, records unsuccessful attempts in an audit log and forces a delay of at least 30 minutes before allowing further attempts.
d) displays a notice warning that the system must only be accessed by authorised users.
e) displays, if possible, after user acknowledgment of the warning notice, the date and time of the previous successful logon, with details of any unsuccessful attempts since then.
f) at the server and applications level, provides Discretionary Access Control (Access Control Lists) implemented by the underlying operating systems, which will restrict the type of access a User may have to an object (files, programs, databases) and the type of operations invoked, i.e., read, write, update and delete operations; and enables the System Owner to grant or change individual users' access rights to specific files.
g) ensures, via automatic lock facilities, that an unused/unattended workstation is locked after a defined period (normally 15 minutes) during which no key depressions are detected.

Access Control for System Operators

Access control rules and rights for system operators will be clearly defined and documented in terms of:

h) Security requirements.
i) Policies for information dissemination and authorisation, e.g., 'need to know' principle.
j) Relevant legislation and any contractual obligations regarding protection of access.
k) Standard access profiles for common categories of job.

Access rights for all administrative functions will be reviewed by the System Operator and System Owner every 6 months and agreed with the IM Security Manager (or equivalent). In the case of Group networks and systems, these will be reviewed by the Group IM Security Manager.

System & Network Management Consoles

Management consoles (i.e., dedicated workstations required for monitoring and maintaining the systems and networks) used by the System Operator will enforce a logon mechanism based on successful entry of a password and associated ID, before access is granted. Management consoles will enforce a timeout mechanism to lock the terminal after 15 minutes of inactivity, after which re-authentication will be required to unlock the console.

Operating System Accounts

Operating system accounts will be under the sole control of the System Operator, with strict password management enforced and the following measures applied:

l) Access to system utilities required to manage operating systems will be controlled and limited to administrators.
m) Users will only be granted the minimum privileges required to undertake their tasks.
n) Audit logs will be implemented, and each audit log file set up as a privileged file with access permitted only through privileged functions.

Network

System Owners and System Operators will ensure the following principles are applied:

o) General access to and from external networks is to be prevented.
p) Access to network analysis and diagnostics tools will not be available generally, unless authorised by Group IM.
q) All unused communications ports are to be disabled and the introduction of unauthorised devices has to be detected.
r) Permanent Dial-up facilities will not be permitted, unless authorised by the IM Security Manager (or equivalent).

Firewalls

System Owners and System Operators will ensure that firewalls are subject to monitoring, with audit logs reviewed for unusual activity, and the following principles applied to firewall rulesets:

s) Incoming ICMP traffic is to be blocked.
t) SMB protocols will be blocked on interfaces to uncontrolled networks and to/from the Internet and linked DMZs, except where specifically authorised by the IM Security Manager (or equivalent).
u) By default, all traffic will be blocked, and ports only opened by exception.
v) Applications requiring access through firewalls shall be designed not to use dynamically assigned ports.

A.9.2 User Access Management

9.2.3 The following password practices will apply to validate users and prevent unauthorised access to information systems:

a) The System Owner will allocate each user-id (which must not give any indication of the user's seniority, i.e., manager, supervisor), keeping a record of user-ids issued, who authorised the issue and when issued.
b) Initial passwords issued to users will be conveyed in a secure manner.
c) Passwords will not be conveyed through electronic mail without protection.
d) Users issued with an initial temporary password will immediately change it to one of their choice that meets the mode's requirements.
e) Users will generate passwords with the following characteristics, i.e., be changed every 40 days; be at least 6 characters in length; and not be commonly used words, names, common acronyms, initials, birthdays, calendar days, months or phone numbers.

A.9.4 Network Access Control

9.4.4 Dedicated private lines, VPN encryption, network user address checking facility or dial-back service will be used to assure the source of connections for remote node authentication.

9.4.7 Apart from firewalls, VLANs and VPNs that are being used to restrict access on shared networks, other security measures will include:

a) No remote accessible diagnostic ports are to be implemented or enabled.
b) All unused ports on local switches and hubs shall be disabled.
c) No modems will be attached to any of the servers or workstations.
d) Access controls at log-on shall protect system utilities from unauthorised access.
e) All communicating entities are to be identified and authenticated.

A.9.5 Operating System Access Control

9.5.5 Measures to be applied to control access to and use of system utilities are described below.

Mainframe and Mini-computer Systems

a) Password protection for system utilities.

b) System utilities, for which authorisation levels will be defined and documented and all usage logged, segregated from applications software.
c) Limiting use of system utilities to a small number of trusted, authorised users.

LANs and LAN-attached PCs

d) Only system administrators will be allowed to use system utilities on LANs and LAN-attached PCs.
e) System engineers will be expected to obtain authorisation from the system administrator before use of system utilities in the course of their work.

Stand-alone PCs

f) Only authorised system engineers (and not system users) will be allowed to load and use system utility programs on stand-alone PCs.

9.5.7 The time-out facility on inactive PCs or terminals should clear the screen and close access to the application after a defined period of inactivity (15 minutes).

A.9.7 Monitoring System Access and Use

9.7.2 The events to be monitored by System Operators include:

a) Invalid user authentication attempts.
b) Abnormal use of user-ids.
c) Logons and logoffs of all users.
d) Activity of privileged users.
e) Access to security system details.
f) Access to resource outside normal hours.
g) Changes to user security profiles.
h) Changes to access rights of resources.
i) Changes to system security configuration.
j) Tracking selected transactions.
k) Attacks on operating systems and firewalls.

A.9.8 Mobile Computing and Teleworking

9.8.1 The following measures will be put in place to mitigate the risk of theft or compromise of mobile computing devices:

a) All portable devices will have the option to have encryption software installed to protect data stored on them.
b) Portable device owners are to ensure that their anti-virus products are up-to-date.
c) All portable devices will have appropriate authentication mechanisms to prevent unauthorised access.
d) No portable device will be attached to any part of the mode's LAN/MAN/WAN without prior approval from the IM Security Manager (or equivalent), or Group IM in the case of interfaces to Group networks or systems.
e) Any portable device that is to be connected to the network will conform to the standards as approved by the IM Security Manager (or equivalent).
f) When connected to any network, there shall not be any additional network connectivity (e.g., connected to a mode's LAN with an active modem-based Internet connection).
g) No portable device will be part of the mode's domain, i.e., all resources will need to be separately authenticated.
h) When connected to public networks, it will be the responsibility of the portable device owner to ensure that appropriate technical measures are taken, for example, by enabling built-in firewalls, to prevent the security of the device being compromised.
i) The owner of a portable device will be responsible for ensuring the data stored on it

is backed up.

A.10.1 Security Requirements Analysis and Specification of Systems

10.1.1 A formal risk analysis methodology, such as CRAMM or CRAMM Lite, may be used for larger projects, while a less formal manual risk assessment methodology may be adopted for smaller projects. The latter will cover the need to:

a) Control access to information and services.
b) Produce an audit trail of selected events.
c) Verify and protect the integrity of vital data.
d) Protect confidential data from unauthorised disclosure, including the possible use of encryption in certain circumstances.
e) Comply with regulatory, legislative or contractual requirements.
f) Take back-up copies of essential business data.
g) Recover from failures, especially for systems with high availability requirements.
h) Protect the system from unauthorised amendment or modification.
i) Enable the system to satisfy the requirements of auditors.

A.10.4 Security of System Files

10.4.1 The following strict controls are to be used when implementing operational systems software in order to minimise the risk of corruption of application systems:

a) Updating of operational program libraries is to be performed only by the nominated librarian, after appropriate authorisation (see 10.4.3).
b) Source code is to be held in a separate source code library.
c) Executable code is to be implemented on an operational system only after successful testing and system owner acceptance, with the corresponding program source library updated to the latest version of the operational system.
d) An audit log is to be maintained of all updates to operational program libraries.
e) All previous software is to be maintained as a contingency measure. Archiving of older versions of application software must be such that it is always possible to revert to an earlier version of any software, if necessary.

Other measures to be considered include:

f) Vendor supplied software used in operational systems should be maintained at the level supported by the supplier.
g) Any decision to upgrade to a new release should take into account the security of the release, i.e., the introduction of new security functionality or the number and severity of security problems affecting the current version.
h) Software patches should be applied when they can help to remove or reduce security weaknesses.
i) Physical or logical access should only be given to third party suppliers for support purposes when necessary, with management approval.

10.4.2 To protect operational data used for testing purposes, the following controls are to be applied:

a) Access control procedures used for the operational systems should also be applied to the test systems.
b) Each time live data is required for testing, the copying and use should authorised and logged to provide an audit trail.
c) After the testing is complete, the operational data copies should be erased immediately from the test system.
d) Test data outputs must be clearly identified and separated from live data outputs.

10.4.3 Other measures which may be considered for Program Source Libraries include:

a) IM support staff should not have unrestricted access to program source libraries.
b) Programs under development or maintenance should not be held within operational program source libraries.
c) Updating of program source libraries and issuing of program sources to programmers should only be performed by a nominated librarian upon authorisation from IM Service Delivery & Support management.
d) Where possible, program source libraries should not be held in operational systems.
e) Program listings should ill be held in a secure environment (see 8.6.4).
f) An audit log should be maintained of all accesses to program source libraries.
g) Maintenance and copying of program source libraries should be subject to strict change control (see 10.4.1).
h) Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, along with all supporting software, job control, data definitions and procedures.

A.10.5 Security in Development and Support Processes

10.5.3 The following restrictions or constraints need to be considered on changes to software packages:

a) The risk that built-in controls and integrity might be compromised.
b) The possible need to obtain the consent of the vendor.
c) Implications for capability of future updates.
d) Responsibility for the maintenance of the software changes.

APPENDIX B: INFORMATION SECURITY REQUIREMENTS (FOR TFL GROUP SUPPLIER CONTRACTS)

B.1 PRINCIPLES FOR SECURITY FOR THE IM SERVICE

B.1.1 The objective is to enable the mode and any outsourced suppliers to provide the IM services, in accordance with Transport for London (TfL) Group Information Management (GIM) security policies, standards and procedures, together with common best practice as described in BS ISO/IEC 17799: 2000 and all relevant laws and regulations.

B.1.2 In particular, the mode and, where used, its outsourced suppliers and TfL shall, prior to the first "go live" date for the IM service agree, implement and comply on an ongoing basis with a security policy and supporting procedures and standards so as to protect TfL's information, assets, networks, systems and staff by:

a) Providing for the confidentiality, integrity and availability of the data and systems making up the service;
b) Ensuring that unauthorised access is not permitted to the data and systems making up the service;
c) Ensuring that the mode and all its suppliers' staff, sub-contractors and 3rd parties involved in the provision of the IM services comply with the security policy and supporting procedures and standards;
d) Implementing effective change controls and tracking of access to the data and systems;
e) Implementing protection against computer viruses and security threats of a similar nature, as well as a means of isolating and removing such viruses from the data and systems used to provide the services;
f) Protecting the TfL network against access via the mode's suppliers' premises, data centres and networks used by the supplier in the provision of the services;
g) Actively monitoring and policing the security of the services for compliance with the security policy, procedures and standards with emphasis on the provision of an audit trail which can be used to detect trends and also to aid in the investigation of security incidents and violations;
h) Providing a forum for the mode's IM and suppliers' security teams to continually improve the security policy, procedures and standards so as to keep abreast of evolving security threats and an escalation point for security incidents and violations;
i) Providing support for TfL's periodic audit or unannounced spot audit of the mode's and suppliers' conformance to the security policy, procedures and standards and the prompt and enduring rectification of any shortfalls identified by such audits or as otherwise brought to the attention of the mode or any of its suppliers by TfL.

B.1.3 Note that TfL may elect to use specialist external IT Security organisations in the execution of any security reviews or audits with the mode or any of its suppliers. A list of approved companies will be maintained by the TfL Group IM Security Manager and made known to the mode and its suppliers, along with any changes to that list which may from time to time be required.

B.2 IM SECURITY POLICY

B.2.1 The IM Security Policy will set out the security measures to be implemented and maintained by both the mode and any outsourced suppliers in relation to all aspects of the Services, including but not limited to the Security Architecture, the IM Services Systems and all processes associated with the delivery of the IM Services.

B.2.2 The IM Security Policy will be structured in accordance with British Standard BS 7799-

2: 2002, cross-referenced to other schedules of any Agreement and call-offs instituted by the mode with an outsourced supplier, where these cover specific areas included within this standard framework.

B.2.3 The IM Security Policy will be amended from time to time throughout the duration of such an Agreement to reflect:

a) new or changed threats and countermeasures

b) emerging Common Best Practice.

B.2.4 The IM Security Policy and all amendments thereto will be agreed with the TfL Group IM Security Manager.

B.2.5 The baseline security levels detailed in Appendix B of the TfL Group Information Security Standard will apply to all modes and their outsourced suppliers, and will form the basis of the mode's Security Policy. The Group Information Security Standard represents the minimum level of security. Individual modes may, where risk assessment suggests, implement more rigorous security measures. Modes must not implement less rigorous security measures without prior approval from the Group IM Security Manager.

B.3 CERTIFICATION TO BS 7799-2: 2002

B.3.1 Both the mode and any outsourced suppliers will provide the IM services in accordance with the standard required by BS 7799-2: 2002 and, in the case of outsourced suppliers, they will use all reasonable endeavours to obtain certification of the Security Architecture to BS 7799-2: 2002 as soon as reasonably practicable and will maintain such certification for the duration of the Agreement with the mode. Subject to the exclusion in the paragraph below, if a supplier fails to provide the IM services as required by this paragraph, TfL may treat such failure as a severity 1 issue.

B.3.2 If certain parts of the Security Architecture do not conform to Common Best Practice security controls, as summarised in BS 7799-2: 2002 and detailed in BS ISO/IEC 17799: 2000, and as a result if a supplier to the mode reasonably believes that its certification to BS 7799-2: 2002 would fail in regard to these parts, TfL may waive the requirement for certification in respect of these parts.

B.4 AUDIT AND TESTING

B.4.1 The Security Policy will be approved and tested, in particular:

a) Testing for service 'go live' date

b) Disaster recovery and contingency testing

c) Services system backup testing.

B.4.2 Adherence to the Security Policy will be monitored through IM Security Management. The procedure manuals and logs produced through the IM Security Management process, which demonstrate such adherence, will be subject to annual audits by an independent party nominated by TfL.

B.4.3 At any time, TfL may require such audit to be undertaken in respect of all or part of the Services and associated processes.

B.4.4 Any breach of the Security Policy by members of the mode's staff, will be treated as a disciplinary offence or any breach by an outsourced supplier will be considered a material breach of the outsourcing Agreement.

B.4.5 The mode and any outsourced suppliers will ensure that the Security Policy is kept up to date with any changes to the IM Services, the System Architecture and associated processes. Any supplier to the mode will deliver the Security Policy and associated documentation within 24 hours of a request by TfL.

ELECTRONIC MAIL
AND THE INTERNET STANDARD

Human Resources

1. INTRODUCTION

It is the policy of London Underground (LU) to set standards to ensure that employees understand how electronic mail (e-mail) and the Internet should be used and to alert employees to the fact that breaches of this Standard may lead to disciplinary action being taken. Where such breaches are deemed to be gross misconduct disciplinary action may result in dismissal.

2. SCOPE

This Standard applies to all LU employees, employees of agencies and consultants who work for LU. This Standard also applies to the use of all of LU's systems, and includes the use of LU's laptops and an individual's own or a third party's computer equipment when they are working on LU's business away from LU's premises (remote working). Employees must comply with this Standard when using LU's e-mail service from any location.

3. REQUIREMENTS

3.1 When using e-mail and the Internet employees must ensure they do not formulate, access, or pass on, material that is defamatory, obscene or which might be regarded as offensive on the basis of personal characteristics such as race, colour, religion, nationality, gender, disability, sexual orientation or age. This includes any material of a sexually explicit nature, which LU deems as offensive. Employees who receive any such material must not forward it on, but must inform their manager or local Human Resources office immediately. Any breaches of these requirements will normally be regarded as gross misconduct and are likely to result in dismissal. A breach of this requirement may constitute harassment and /or may be unlawful.

3.2 E-mail and the Internet are uncontrolled environments and should not be regarded as secure systems. Employees must therefore exercise extreme care when sending confidential or sensitive material by e-mail. When downloading information, employees must take care to avoid the introduction of viruses or the infringement of third party copyright or licensing requirements.

3.3 Software programs must not be downloaded from the Internet on to a desktop computer. Staff must ensure that floppy disks or CD-ROMs which are to be used on any of LU's systems are virus scanned before being used. This includes any

disks supplied via professional or any other bodies.

3.4 Limited personal use of e-mail and the Internet may be allowed, provided such use is kept to a reasonable level, does not interfere with an employee's performance in carrying out their duties, does not have a negative impact on LU in any way, and is lawful and adheres to the principles contained within this Standard. Employees are reminded that LU reserves the right to monitor and/or record individual e-mail and Internet use for its lawful business purposes. Employees should therefore have no expectation of privacy whilst using company equipment for the purposes of communicating via e-mail or in accessing or passing on information obtained through the Internet.

3.5 E-mail and the Internet must only be accessed via the user's personal user account and employees must not attempt to use another user's account without their prior expressed permission.

4. RESPONSIBILITIES

All Employees:

- To comply with this Standard.

All Managers:

- To ensure that the requirements outlined in this Standard are enforced in their areas of responsibility, and that appropriate fair and consistent action is taken to deal with any failure to conform to them, in accordance with the appropriate procedures.

General Manager HR:

- To review the effectiveness of this Standard and audit compliance with the requirements stated therein.

5. SUPPORTING AND OTHER RELEVANT DOCUMENTS

Company Employment Policy
Discipline Standard
Code of Conduct Standard
Workplace Harassment Standard

Transport for London

Requirements for issue and use of mobile telephones and pagers

Purpose

The purpose of this Standard is to detail the requirements to be followed by all managers who authorise the issue or use of mobile telephones and / or pagers. It is designed to improve efficiency, ensure best value for money procurement and encourage responsible stewardship of Company resources by applying reasonable controls on the issue and use of mobile telephones and pagers. It is not intended to be over onerous on managers or restrictive on staff; suitable support and advice will be provided by procurement and Telephone Services.

Scope

This Standard applies to all TfL / London Underground staff and staff employed by TfL / London Underground who have or use a Company issued mobile telephone and / or pager. This Standard shall be enforceable from 1st April 2003.

Requirements

Entitlements to mobile telephones and pagers The annual spend on mobile telephones and pagers within TfL / London Underground is significant and has increased dramatically over the last few years. In view of this trend it is essential that the issue and use of mobile telephones and pagers be controlled in an appropriate manner. To this end mobile telephones and / or pagers should only be issued to staff if: ·

- Their duties require them to work away from a fixed site of work for lengthy
- periods of their working day
- They have critical customer or supplier relationships that necessitate an immediate response to their enquiries
- They are required to be "on call" on a regular basis and are required to be contactable on TfL / London Underground business outside of normal hours or when not at their usual site of work

If the nature of a member of staff's work changes and no longer meets one of the above criteria, then the mobile telephone and / or pager must be returned to Telephone Services immediately.

Business calls

Mobile telephones are only to be used by members of staff for business purposes when no cheaper alternative (e.g., land line, e-mail) is available. Certain numbers will only be permitted by exception where a specific business need can be demonstrated; in all other instances these numbers will be barred by Telephone Services. Examples of barred numbers may include, but are not restricted to, international calls and premium rate calls. If access to these numbers is required, a request must be approved by a General Manager or Director and submitted to Telephone Services. If individuals use private mobile telephones to conduct business related calls they may claim back any expenses incurred in the usual manner. If the volume of calls rises to a significant level individuals will be issued with a company telephone.

Private Calls

TfL / London Underground provides mobile telephones for Company Business, and the use of mobile telephones for private use should be minimised and restricted to exceptional circumstances such as emergencies or unforeseen schedule changes. If excessive private calls are made the Company will require reimbursement for the cost incurred. Procurement will periodically provide managers with a review of the cost information for mobile telephones used by their staff. Where, in the manager's opinion, excessive private use has occurred they should initiate a recovery procedure for the amount from the individual concerned.

Procurement of mobile telephone and pagers

All mobile telephones and pagers must be ordered via Telephone Services. All applications must be made on an "Application for Telephone Equipment" form, which can be obtained from Telephone Services, until a method for applying via the intranet is developed. Telephone Services will ensure that the correct level of authorisation is provided on the application. Telephone Services will provide a standardised "appropriate model" suitable for general business purposes unless a specific business case is made for a handset that exhibits data compatibility or tri-band functionality. Any such business case must be approved by a General Manager or Director and be submitted to Telephone Services. The "appropriate model" will be based upon the most cost-effective solution available at the time. In accordance with the Stewart Report on Mobile telephones and health, consideration will also be given to the Specific Absorption Rate (SAR) value of the telephones supplied. Only standard text pagers will be issued.
The procurement of mobile telephones and pagers will be via tendered contracts to ensure best value for money is achieved. The contracts will be let in accordance with TfL / London Underground's purchasing rules.

Billing

TfL / London Underground will implement electronic billing for mobile telephones and pagers wherever possible. This not only minimises unnecessary administrative work, but also provides the detailed cost information required by

procurement and management to monitor costs and ensure policy compliance.

Upgrades to mobile telephones

Upgrades to mobile telephones will only be provided if the use of the mobile telephone changes and that the change requires a different model of handset. Upgrades can only be authorised by a General Manager or Director. Before an upgrade is issued the old handset must be returned to Telephone Services and the new handset signed for. Telephone Services will again ensure that the correct level of authorisation is provided.

Disposal procedures

Disposal of mobile telephones and pagers should be via Telephone Services. Telephone Services will ensure that the assets are disposed in an environmentally responsible manner or re-issued as appropriate and ensure that any airtime agreements are cancelled.

Mobile telephones and IM

There currently is some confusion surrounding mobile telephones and TfL / London Underground's IM systems. Customers have ordered equipment from Telephone Services with the expectation that they would be able to connect this equipment to their PC or to use it to access their mail or calendar.
There is a large variety of mobile telephone equipment on the market and the list is growing. Models tend to have a fairly short product life and are quickly superseded. Any software supplied with the telephone tends to be proprietary to that particular model or range.
To ensure the integrity of TfL / London Underground's IM systems, all software and hardware that requires connection to the IT network or to the desktop PC has to undergo reasonable risk assessment and ideally be "Model Office" tested against the standard environment. This is a costly and time-consuming exercise, but vitally necessary to protect existing systems.
At the present time there are no mobile telephones or combination telephones and PDA's (such as the Nokia 9210i), which are approved for use with the TfL / London Underground IM infrastructure

Specifically, this means that:

1. TfL / London Underground IM does not facilitate or support the connection of any mobile telephone to a company PC.
2. TfL / London Underground IM does not facilitate or support the connection of any combined mobile telephone / PDA (such as the Nokia 9210i) to a company PC.
3. TfL / London Underground IM does not facilitate or support the connection of any combined mobile telephone / PDA (such as the Nokia 9210i) to the London Underground network via RAS.
4. With the exception of Street Management, GPRS cannot currently be used to access any TfL / London Underground IM system

When a customer requests a mobile telephone other than the 'standard' variety, they

should be advised of the above to ensure that they are not disappointed. The IM department is, however, investigating solutions that will provide wireless access to the TfL / London Underground network and ways of connecting mobile telephones which mimic existing PALM and PocketPC PDA's to company PC's. The best advice that can be given to users is that if they are considering procuring a mobile telephone to meet an IM related requirement then they should in the first instance be directed to IM Change on auto 1222 who will capture the requirements and investigate possible solutions.

Responsibilities

Authorisation

A General Manager or Director must approve all mobile telephone applications. A Manager, Business Manager, General Manager or Director must approve all pager applications.

Monitoring of costs

Procurement, in conjunction with accounts payable, will periodically perform a random independent assessment of costs incurred by mobile telephone users in each cost centre on behalf on the cost centre owners and will liase with the relevant managers if costs are considered to be excessive, based upon the anticipated usage. If cost reductions are required then appropriate action should be taken to reduce future expenditure, reclaim costs and assess if mobile telephone requirements are the most appropriate means of communication for those members of staff.
Procurement will also assist managers in performing an annual audit of all mobile telephones and pagers in use across the business. If procurement believes the service provider has incorrectly raised tariffs, Telephone Services should be informed, who will raise the concern with the service provider directly.

Ownership of mobile telephones

Before a mobile telephone can be issued to a member of staff, the relevant party must sign for the handset and any other equipment to be issued (e.g. charger, hands free kit). Where departmental, or pool telephones are required, an appropriate party must assume overall responsibility for all such assets. The mobile telephone and other equipment issued remain the property of TfL / London Underground at all times. In the event of loss or damage the member of staff is responsible for covering any costs incurred except in the case of theft, where a crime number must be obtained from the police before a new mobile telephone will be issued.

Managers must ensure that any member of staff leaving TfL's / London Underground's employment returns any mobile telephone or pager to Telephone Services to avoid liability for all ongoing call and rental charges. HR will require verification from telephone services that all telephony equipment issued to an employee has been returned before final salary payments are made. This verification can be in the form of a completed checklist signed by a member of telephone

services.

Assets should not be re-issued locally but in every case where a mobile telephone or pager is no longer required it must be returned to Telephone Services for subsequent re-allocation or disposal as appropriate.

Health

The Stewart Enquiry into mobile telephones and health determined that:
"The balance of evidence does not suggest mobile phone technologies put the health of the general population of the UK at risk. Preliminary evidence suggests some cases of subtle biological effects but these do not mean health is affected."
However prudence recommends that:

- Mobile telephones should be used for as short a time as possible.

- Only mobile telephones with low SAR values should be used.

IM Policy

Group Information Management
Ref: IM/TA.01/P01-R1.0
Issue date: February 2005
Effective: February 2005
Amended:

INFORMATION SECURITY

Title

Information Security **including**

- Management
- Organisation
- Risk
- Compliance

1. Purpose

The objective of this policy is to ensure that TfL Group companies and employees maintain a level of information system security, information integrity, as well as privacy practices commensurate with that required to mitigate the risk of information misuse, damage or loss. It also aims to ensure TfL's compliance with statutory, regulatory and contractual security requirements in its design, creation, operation, use and management of information and information systems.

2. Definitions

GIM means Group Information Management

Information or 'data' in context refers here to information of any kind and used in any way in a business unit system. Examples include electronic messages, communications, emails, files, records, images, graphics, transmissions, programs, software and data.

Information owners are senior business unit managers with the authority for acquiring, creating, maintaining and disposing of information and information systems within their assigned area of control.

Information custodians are individuals (i.e. staff within Information Management departments or system administrators) in physical or logical possession of information from Owners, and are charged with the provision of information systems and security services to the Owner.

Information users are TfL employees, temporaries, contractors, consultants or other third parties with whom special arrangements (such as confidentiality and

non-disclosure agreements) have been made. All Users must be known to and authorised by custodians.

Information system refers to an information based organisational capability and as such not only includes the data and information in all media, hardware, software and supporting networks to the processes and human resources that supports its acquisition, storage and communication.

Information Security (IS) is defined as the ability to protect the integrity, availability, and confidentiality of information held by an organisation and to protect IT assets from unauthorised use, modification, accidental or intentional damage or destruction.

Information Security management system is the processes used by TfL to identify the assets to be protected, the approach to risk management, the control objectives and controls (inclusive of policies) and the degree of assurance required.

Security refers to Information Security

Transport for London (TfL) – refers to all parts of the TfL Group, that is its business units, associated entities and any part of Group identified by the Greater London Authority Act 1999

TfL Group: TfL and its subsidiary organisations and their own subsidiaries. References to a 'subsidiary' of TfL will include a subsidiary of a subsidiary of TfL unless otherwise stated.

Trusted environment describes the physical and logical boundaries of the information infrastructure within which the confidentiality, integrity and availability of TfL's information assets are assured through the enforcement of its information security management system.

3. Organisational scope

To be effective, information security must be a pervasive effort involving the participation and support of every TfL employee who deals with information and /or information systems. This policy applies to all information in all media, computer and network systems owned by and/or administered by TfL, as well as those provided and supported through contractual agreements with 3rd party service providers. It applies to workers at TfL, no matter what their status (employee, contractor, consultant, temporary, volunteer, intern, etc.).

4. Policy statement

TfL is critically dependent on both its information and information systems in achieving its strategic vision. If confidential TfL information were disclosed to

inappropriate persons, become unavailable or unreliable the company could suffer serious financial, commercial or legal damage.

This policy defines the baseline information security control measures that all users in TfL are expected to be familiar with and to consistently follow. These security measures are the minimum required to prevent a variety of different information security problems. The policy therefore specifies the minimum level of due care to be taken by all TfL Group companies, and employees.

5. Policy content

This Information Security policy mandates that all TfL companies take the necessary steps to initiate and manage an enterprise-wide approach to Information Security management, consistent with those outlined in best practice industry standards for Information Security management such as the ISO/IEC 17799 code of practice.

Ownership for the security of TfL information assets lie with the Director, Group Information Management whose duty is to ensure that all Information Owners, Custodians and Users are made aware of this policy, and that all staff or workers observe it when engaged in TfL contracts.

5.1 Information Security management

The Head of Information Management (HIM) in each TfL business unit company is responsible for the development, enforcement, management and maintenance of Information Security, and shall deploy the necessary controls to demonstrate compliance of Information owners, custodians and users to the Group Information Security Policy requirements.

- Responsibility for IM Security will be assumed by the Director Group Information Management for any business unit without a HIM.
- Information owners within each TfL business unit are responsible for ensuring that the business unit operate in a manner consistent with the maintenance of a shared, trusted environment within the TfL information network.
- Each Head of Information Management is responsible for ensuring that agencies and third parties with which they are engaged contractually to provide information or information services, within the framework of these contracts, also comply with this requirement for the protection of TfL's data.
- Whereas TfL business units may establish certain autonomous applications & systems, including those hosted or managed by a third party outside of the shared trusted environment, the information owner shall liaise with the HIM to ensure that the establishment and operations of these application will not jeopardise the enterprise security environment, specifically:
    - The security protocols (including means of authentication and authorisation) relied upon by others and

- The integrity, reliability and predictability of the TfL backbone network.

- Each TfL business unit must subscribe to the following principles of shared security to be enforced by the business unit's Head of Information Management, and shall:
  - Follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels.
  - Ensure secure interactions between and among TfL group companies take place within the shared and trusted environment.
  - Ensure secure interactions between and among business partners, government agencies and other external parties through common authentication process and security architecture.
  - Prevent misuse of, damage to or loss of IT hardware and software facilities.
  - Prevent unauthorised use or reproduction of copyrighted material by public entities.

- Changes to this or supporting policies, standards or guidelines will be managed through the Group Governance change control process.

5.2 Information Security organisation

- Information Security is a business responsibility shared by all members of the management team. As part of this management body a Group Information Security Forum shall be established to ensure that there is clear direction and visible management commitment to information security within TfL.

- The IM Steering Group will function as the business management group for Information Security.

- The Heads of Information Management will function as the delegated operational management group for Information Security.

- Heads of Information Management Group shall designate internal responsibilities for management of information security within the business unit who shall ensure local compliance with the Group Information Security policy and standards for secure operations within the TfL trusted network.

- The Group Information Security manager has overall responsibility for the development and enforcement of security across the business units.

5.3 Risk management

- Risk management describes the process of identifying, controlling, minimising and/or eliminating security risks that may affect TfL's information systems, for an acceptable cost. The assessment of information risk is the responsibility of the Information owners within each business unit, and the Heads of

Information Management shall manage these risks through the enforcement of the Group Information Security policy and standards.

- Where an exception to Group Information Security policies or standards is deemed necessary, a formal case for waiver must be submitted to the Heads of Information Management. Waivers will include a full acceptance of risk by the requesting Information owner.

- Waivers will only be granted by the Heads of Information Management, acting through the Director Information Management on advice of the Group Information Security Manager. Only temporary waivers may be granted after the agreement of risk acceptance by the Information owner.

- A formal review of waivers will be done by the Group Information Security Manager on a half-yearly basis. The Group Information Security manager will address waivers requiring review and renewal within a much shorter timescale on a case by case basis.

5.4 Incident handling and response

- Heads of Information Management shall ensure local enforcement of security monitoring and incident response procedures and shall co-ordinate with HR to ensure that information users are made aware of, through education and training, the procedures for handling and reporting information security incidents.

- Information users must be able to identify security breaches and the process for reporting infractions to assigned security personnel through established channels.

- In addition, employees shall be kept apprised of the latest security risks as well as any changes to corporate security practices through communication/notification from the Heads of Information Management within each business unit.

5.5 Compliance

- Compliance with the Group Information Security Policy is enforced through a Group Internal Audit process.

- Heads of IM within each TfL business unit are responsible for the oversight of their respective information systems security posture, and will confirm in writing that the TfL Business Unit is in compliance with this policy.

- Each TfL business unit shall review its IM security processes procedures and practices annually and make the appropriate updates after any significant change to its business, computing or networking environment. This review shall be sponsored by the local Head of Information Management.

- Each TfL business unit must maintain documentation showing the results of its review or assessment, and the plan for correcting deficiencies revealed by the audit.

    - The TfL Group Auditor will perform a periodic audit of the TfL security processes, procedures and practices for compliance to this policy.

6. Procedures

Detailed advice and guidance on the procedures to be followed in the implementation of this policy lie with the Head of Information Management responsible to delivering the information or information system service within the TfL business unit.

Change procedures for the modification or amendment of this policy are documented in the change control procedures and are available online on the TfL Group Information Management web site.

7. Approval amendments

This policy was approved by the Chief officers on 18th February 2005 .

8. Review

Technological advances and changes in the business requirements of subsidiaries will necessitate periodic revisions to policies, standards, and guidelines. Group Information Security Manager is responsible for routine maintenance of this policy to keep it current. As such a review of this policy will be undertaken whenever circumstances warrant. Notwithstanding any interim review the policy will be reviewed annually.

9. Policy owner

The Director Group Information Management is the designated owner of this policy.

10. Contact details

For advice and guidance on the contents and implementation of this policy contact the following:

- **Group Information Security**
  Group Information Security manager
- **Change Management**
  Group Governance & Strategy manager

11. Related policies/documentation

Group Information Security Standards
ISO/IEC 17799

SCHEDULE 10 - BENCHMARKING

1. Introduction

All defined terms referred to in this Schedule are defined in **clause 1** of this Agreement or **Annex A** of this **Schedule 10** Both Parties agree that they wish to achieve the Benchmarking Objective. The benchmarking shall be undertaken at most annually commencing on the first anniversary of this Agreement Commencement Date.

2. Benchmarking Methodology

2.1 Benchmarking assessments of the Charges in respect of each of the Constituent Services will be conducted by the Service Provider with the approval and consultation with TfL unless the Service Provider wishes to select a qualified, independent, third party to conduct the Benchmarking, with prior approval of TfL and whose fees and expenses shall be paid by the Service Provider.

2.2 Benchmark timetable

The timetable for the benchmarking assessment will be agreed by the parties in writing in advance .

2.3 All issues in respect of the benchmarking process shall be resolved, to the extent reasonably practicable, and a reasonable period of time will be afforded for these considerations prior to the issue of the final benchmark report.

2.4 For the purposes of a benchmark review the terms of reference to be used by the Service Provider shall be agreed by the parties prior to the commencement of the Benchmarking.

2.5 The benchmarking assessment shall be conducted by applying the following general principles and criteria:

2.5.1 Benchmarking assessment shall be carried out in an independent and objective manner.

2.5.2 Benchmarking assessment shall be truly comparative comparing like with like in respect of the Constituent Services to the Office of Government Commerce ("OGC") rates that in the reasonable opinion of the Parties shall be fair comparators for the purchase of the Constituent Services.

2.6 The benchmark comparison will look at the full contract price as TfL's Charge for each Constituent Service and will compare this with the rates published by the OGC for the particular Products and Services on a like for like basis. For the avoidance of doubt any price comparators shall be based on the Charges. These Charges shall include items such as account and service management and the credits set out in section 1.4 of Schedule 6..

2.7 The extent to which any rates referred to in paragraph 2.6 above are not available should be stated in the Service Provider's report.

2.8 The Service Provider's data from the OCG used to make the benchmarking assessments shall be as current as possible and, in any event, no more than eighteen (18) months old, unless both Parties agree upon a longer period.

2.9 Prior to the initiation of the benchmark assessment, both Parties shall agree in writing upon any comparison methodology and adjustment factors which are required in order to take into account any differences between the OGC rates and TfL, such as:

2.9.1 any constraints imposed by TfL on the Service Provider in the provision of the Constituent Services;

2.9.2 market changes; and

2.9.3 the currency and level of detail of the comparative data.

2.10 The Service Provider shall allow TfL a period of twenty one (21) days after collation of the benchmarking assessment data, which shall be prior to the conclusion of the benchmarking assessment analysis, to verify that this exercise has conformed to the agreed-upon methodology and to raise any concerns with the Service Provider who shall consider them in good faith. The Service Provider shall share with both parties in an even-handed manner all data related to the benchmarking assessment and its results to the extent that it is lawfully able to do so.

3. Benchmarking Results and Consequences

3.1 The Service Provider shall report the results of the benchmarking assessment in writing to TfL.

3.1.1 If the result of the benchmarking indicates that the Charges do not meet the Benchmarking Objective then the Service Provider must, within thirty (30) days of the date of the benchmark report, propose a benchmark improvement plan. This plan will detail how the Service Provider proposes to improve the Charges to meet the Benchmarking Objective. The Service Provider will consult with TfL's Contract Manager to discuss possible solutions. The proposed solution documented in the benchmark improvement plan must be based on one of the following solutions:

3.1.1.1 improved or additional services or technology;

3.1.1.2 a reduction in the Charges;

3.1.1.3 any other value adding or value creating initiative to TfL;

3.1.1.4 any combination thereof.

3.1.2 Within seven (7) days of receipt of the Service Provider benchmark improvement plan TfL will enter into discussions with the Service Provider, with a view to agreeing a solution to the issues identified in the benchmark. In the event that the Parties are unable to agree on a solution within fourteen (14) days of receipt of the benchmark improvement plan or sixty (60) days from the receipt of the benchmark report if no benchmark improvement plan is provided by the Service Provider (or a solution is agreed, but not implemented in the agreed timeframes), then either party can terminate this Agreement on 3 months notice to the other party and during this 3 month period the Charges and the Services will remain unchanged.

3.1.3 In the event that both Parties agree on a solution, then the Service Provider will implement that solution as agreed.

3.2 Any benchmark improvements shall be conducted as a project at no charge to TfL.

3.3 TfL reserves the right to undertake a due diligence process on any benchmarking assessment.

3.4 In the event that TfL terminates this Agreement pursuant to clause 3.1.2 if this Schedule 10, TfL shall pay the Termination Charges set out in section 4 c) of Call-Off Contract No. 1 if applicable.

4. Evolution of Benchmarking Processes and Procedures

Both Parties acknowledge and agree that during the Term with advances in technology, tools and expertise in benchmarking, this Schedule may, by agreement between both parties, be revised in line with the prevailing most effective means of conducting benchmarking.

Annex A

Benchmarking Methodology	The benchmarking process to be carried out by the Service Provider and broadly defined in this **Schedule 10**
Benchmarking	A benchmarking exercise carried out pursuant to this **Schedule 10**
Benchmarking Objective	The defined and agreed objectives of the benchmark are to assess, compare and report on the Charges for the Constituent Services according to this Schedule, and if applicable to proceed as set out in paragraph 3.1.
Constituent Services	The entire scope of the Products and Services provided to TfL by the Service

Provider

SCHEDULE 11 - BUSINESS CONTINUITY

The Service Provider will maintain a Business Continuity Plan (the "BCP") to provide continuity of service including therefore continuity of the Services to TfL in the event of systems or infrastructure failure.

The Service Provider's BCP documentation shall be updated quarterly, and audited testing of the BCP shall be carried out at regular intervals.

The Service Provider's BCP shall provide the capability, processes, procedures and plans to minimise the effects of a serious network-affecting incident and to enable the timely restoration of Service(s) in the event of such an incident occurring. Risk assessments shall be carried out on all areas of the Service Provider's core network operations to ensure that changes to the network architecture or configuration do not place the Service Provider network in a position where failure could result, particularly with regard to potential single points of failure and the BCP shall address areas of risk identified.

Service Continuity

The BCP shall be designed to minimise the impact of failure of the Service Provider's network and therefore the Services by the provision of either resilience or redundancy (whichever is most appropriate) within the core Service Provider's network.

In the case of resilience, the objective shall be to design and build in defined levels of additional equipment and transmission capacity which allow the Service Provider's network to continue near-normal operations even in the event of a worst-case scenario such as the loss of an entire network switching centre.

In the case of redundancy, critical Service Provider's network elements shall be fully duplicated in different areas of the country, and while they operate independently during normal operation, each shall be capable of taking over the full load of the other under failure conditions.

Service continuity is a core Service Provider's network design principle, all changes and new additions to the existing Service Provider's network architecture, including all new products and services shall take account of either resilience or redundancy in their design and implementation, and this shall be demonstrated prior to being brought into service.

Service Restoration

The BCP shall assume that a serious service providers network-affecting incident occurs, materially impacting a large geographical area.

The BCP shall include a series of service restoration plans, procedures and processes to be used in such an event.

There are two main areas of documentation:

The restoration plans, procedures and processes themselves shall be contained in a manual which shall be issued to all primary and deputy members of the Service Provider's restoration team in both paper format and in encrypted electronic format. This document shall also contain contact details used by the Service Provider's Network Management Centre for alerting the team members.

The high-level Service Provider's network information used in the restoration process shall be also recorded in encrypted electronic format and include equipment layout, distribution and connectivity diagrams, and detailed coverage information for all of the Service Provider's network switching centres.

Much of this technical documentation is sensitive in nature, and for this reason it is not made available outside the restoration team itself.

Monitoring and management of the Service Provider's network shall be carried out from two geographically separated Service Provider's network management centres.