Appendix 1

Principles of the London Underground Public Wi-Fi Operational Agreement

Glossary

Best Practice Change Management	Proven Change activities and Change processes that have been successfully used by multiple organisations.
Change Advisory Board	A group of people that advises the Change Manager or Authority in the Assessment, prioritisation and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, the Business, and Third Parties such as Suppliers
Change Approvers	The persons with the authority to approve a change, usually a member of the Change Advisory Board (CAB)
Change Policy and Processes	The Policy that governs the approach to Change Management and the Change Management process detailed in the Operational Agreement
Configuration Item (CI)	Any Component that needs to be managed in order to deliver the Service
Configuration Management Database (CMDB)	A database used to store Configuration Records throughout their Lifecycle
Controlled Shut Down	The managed interruption of the Service, which would be activated during a security incident
Customers	The general public who pay the Concessionaire to use the Service
Customer Service Contact Centre	The team which will receive contact from customers who will use the Service
Down Time	An agreed period of time when Service can be interrupted during a Planned Change window
Emergency Planned Change	A Change that must be introduced as soon as possible. For example to resolve a Major Incident or implement a Security patch
Fault Incidents	An unplanned interruption to the Service or a reduction in the quality of the Service
Incident Management	The Process responsible for managing the Lifecycle of all Incidents. The primary Objective of Incident Management is to return the Service to users as quickly as possible
Infrastructure	WLAN equipment installed, owned and maintained (or to be installed, owned and maintained at any time during the Term) by or on behalf of the Authority at the Locations for use by (i) the Concessionaire in the provision of the WiFi Service and (ii) the Authority and/or such other third parties as may be authorised from time to time for non-commercial purposes by the Authority, as such infrastructure is more particularly described in the Infrastructure Specification
Network Components	The hardware used to provide the infrastructure for the Service
Network Management	The remote access to the elements of the service directly provided by the Concessionaire, such as, but not limited to; Portal Access and access to the Internet
Operational Agreement	The Document used by both parties which will detail all the

	required processes and procedures needed to support the Service.
Operational Document	The Document which becomes the Operational Agreement that details the processes which will be in place between both parties to operate the Service
Out of Traffic Hours	The time slot in which no trains run across the underground train network
Planned Change	A pre-approved piece of work that follows a Procedure or Work Instruction scheduled to take place during a pre-agreed Change Window.
Problem Management	The Process responsible for managing the Lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening, and to minimise the Impact of Incidents that cannot be prevented
Ready for Service.	A Location is tested and commissioned and is accepted as ready for Public WiFi use by both Parties.
Remedy Fault Management Process	Fully integrated ITIL based Incident Management and Problem Management application
SLA	The Service Level Agreement which will define Quality of Service and the metrics used to measure the service and the remedies in place for not achieving the Service
Service Desk	The Single Point of Contact between the both parties. A typical Service Desk manages Incidents and Service Requests.
Public Wi-Fi Service	The public access WLAN service for broadband internet services and data access to be provided by the concessionaire at Locations pursuant to the Agreement

1. Scope

These Operational Principles will clearly define the separate responsibilities of the Authority's and the Concessionaire's operational teams and the required interactions between them.

The overriding principle is to ensure that

1. The Authority has complete responsibility for the operation of the Infrastructure and its own Authority Services.
2. The Concessionaire has the information and support it needs in order to deliver its own Public Wi-Fi Service as granted through the concession.

This document will address the following areas focused on what is required for the Concessionaire Public Wi-Fi Service:

The Network Management service

- Incident handling and hand off
- Managing change
- Escalations
- Disaster Recovery situations
- The process for bringing stations into support into the live supported environment
- Increases in bandwidth. Process for adding and removing Locations
- Change
- Readiness for Service
- Security breaches, notification and handling
- Controlled Shut Down (i.e. when requested by police) & graceful resumption
- Contact methods

Customer Feedback & Performance Management

- Directing customers to the Concessionaire / Our partners Global Reach/Wholesale partners
- Training & awareness of the Authority's staff
- Example reports
    - from the Concessionaire to the Authority
    - from the Authority to the Concessionaire

It is intended that this document will give the principles and identify the key dependencies required to run the service and will expand into a full Operational Document with details once the concession has been awarded and the operational teams can meet to complete details such as contact details and agree response times.

The target date for both the Concessionaire and the Authority to agree the full Operational Document will be the 1st May 2012.

- Where the SLA is referenced this will be agreed and documented in Schedule 11 of the Agreement.

Bandwidth increases:

- The process for requesting increases in bandwidth and appropriate justification shall be agreed based on the following principles:
  - Bandwidth increases to be implemented in 100Mb
  - Justification for bandwidth increases is required. Bandwidth increase requests should not be unreasonably withheld or delayed.
  - Changes will be in accordance with Clause 32

Readiness for Service:

The Authority and the Concessionaire will agree the following acceptance criteria for each Location where the Concessionaire's WiFi Service is deployed.

The tests undertaken do not need to be limited to the following, however the following represents the minimum criteria to be agreed by both Parties for a Location to be deemed 'Ready For Service'. Both Parties must provide signed acceptance, acceptance not to be unreasonably withheld or delayed.

1. The Location has been registered with both Parties Service Desk functions.
2. A series of tests under project governance have been agreed and executed and both Parties have agreed the outcome of those tests.
3. The Authority and the Concessionaire both agree that the adequate monitoring tools are in place, sufficient for the Location to be deemed 'Ready for Service'

Once the Location has been accepted into service the number of AP's at that Location will be validated against the initial design and the table in Schedule 3A updated.

2. Incident Log & Pass Procedure

This process will define how the TFL IM Service Desk and the Concessionaire's Service Desk will interact and communicate between each other during Fault Incidents and how Problem management will be conducted.

An example Incident Management process is detailed in Appendix A. The Agreed Incident Management process will be document in the Operational Agreement.

It is fully understood that there are strict access limitations within the underground network and these will be taken in to account when agreeing the Service Level Agreement metrics between both parties.

Principle:

The Concessionaire is focused on the service to the customer of the Concessionaire Public Wi-Fi Service.

The Concessionaire's Service Desk will be the single point of contact for all Fault Incidents related to the Concessionaire Public Wi-Fi Service.

Service Desk will log all instances relating to the Concessionaire's Public Wi-Fi service into our Remedy Fault management system and investigate with all resolver groups in the Authority including the TFL IM Service Desk and other partners who provide elements of the Concessionaire's Public Wi-Fi Service.

Examples of typical WiFi Infrastructure incidents which may occur on the Authority's WiFi Infrastructure:

Faulty Access Point

Resolving Group: TFL IM Service Desk.

The Concessionaire would expect TFL IM Service Desk to also:

Notify the Concessionaire's Service Desk so that Concessionaire can log and manage the information flow to the Customer Service Contact centres in order to deal with calls from the Public WiFi Customers.

Provide an escalation route if the Access Point is not repaired within the agreed SLA.

Station out service

Resolving Group: TFL IM Service Desk.

The Concessionaire's Service Desk would expect TFL IM Service Desk to:

Notify the Concessionaire's Service Desk in order for Concessionaire to log and manage the impact of this to the Concessionaire's Public Wi-Fi Service.

Provide an escalation route if the access station is not returned to service within an agreed SLA.

Example of Customer Feedback issue

Large number of customer notifications via Concessionaire's Customer Service Contact Centre causing Concessionaire to investigate loss of service.

The Concessionaire's Service Desk would commence investigation

The Concessionaire's Service Desk would expect to be able to log an Incident with the TFL IM Service Desk

TFL IM Service Desk to investigate and respond in accordance to an agreed process

The Concessionaire's Service Desk would then liaise with the relevant resolver groups and customer touch points until resolution.

The Concessionaire's Incident Management approach to the Wi-Fi Public Service

Incidents can be raised by the both TFL IM Service Desk and Concessionaire's Service Desk.

Incidents will be logged on the Fault management system which manages the incident against the agreed SLA.

The Concessionaire's Service Desk investigate the incident including contacting the TFL IM Service Desk via the agreed Incident management process.

Service Desks will agree the SLA for each type of incident which will be prioritised based on the severity that the service is impacted. Concessionaire proposed prioritisations follow however we expect to discuss and agree these with the Authority following the award of the concession.

Example Prioritisations Table

Priority	Example	Action
1	Major Service Outage affecting service at multiple stations	
2	Major Service Outage affecting service at a single station	
3	Minor Service Outage affecting part of a station, e.g. a platform	
4	Minor Service Outage, e.g. single Access Point out of service	

3. Requirements of the Authorities Operational team:

The Concessionaire's Service Desk will require TFL IM Service Desk support to liaise with in order to raise Incidents for investigation within an agreed SLA depending on the severity of the service issue.

TFL IM Service Desk will log a support call on their fault management system and issue an Incident reference number (ticket) to the Concessionaire's Service Desk

The Concessionaire's Service Desk expects the TFL IM Service Desk to have direct access to the resolver group which has the ability to remotely access the infrastructure devices in order to investigate and identify possible causes of incidents.

An Escalation process will be required in the event of the Concessionaire's Service Desk not being able to contact the TFL IM Service Desk.

The agreed formalised Incident Management Process will be documented in detail in the Operational Agreement.

An example Incident Management process is detailed in **Appendix A**

4. Change Management

TFL IM Service Desk are required to notify The Concessionaire's Service Desk of Planned Changes, including Emergency Planned Changes, when the change affects or places 'at Risk' Service to the Concessionaire's Public Wi-Fi Service.

This process will detail the Change Management processes and Planned Outage process between all parties, including notification periods and preferred Change windows. The agreed finalised Change Management processes and Planned Outage process will be detailed in the Operational Agreement.

Preferred windows for service affecting changes will be out of the Authority's Traffic Hours between 01:30am and 04:30am.

Should there be a need to extend these hours due to an event such as New Years eve, the Olympics or any other major event by prior notice then this will be managed by the change control process.

Down Time occurred during periods of agreed Emergency and Planned Change will not be included within SLA calculations.

Examples of a change within the Authorities Infrastructure.

Principle:

A change is defined as any alteration of or addition to existing hardware, existing software Network Components and any events that have the potential to impact our ability to maintain services to customers. This also includes changes by suppliers that impact our network.

Such changes may either directly or indirectly affect the operation of technical systems or services (internal or external). All such components are known as configuration items and are stored within the Configuration Management Database. Change Approvers for each item are pre-defined within the CI record

A Change Policy and Processes will be incorporated in to the Operational Agreement

The purpose of the policy is to define the guidelines/principles that need to be followed for the Change Management process.

The objectives of the Policy are to:

- Provide detailed information about the rules surrounding the Change Management Process;
- Describe how the process fits into the relevant Concessionaire and the Authority's contexts;
- Document the roles & responsibilities of all parties involved in the process;
- Clearly define the criteria of what constitutes a "Change";
- Ensure that Changes are managed in line with the Change Management process;
- Remove any ambiguity / jargon surrounding the process.

Scope

This policy and supporting standards shall apply to:

- All of the Concessionaire's employees, contractors and third-party organisations and business partners working in support of the concessionaire and the Authority within relation to the Concessionaire Public Wi-Fi Service
- All of the Concessionaire's infrastructure in relation to the Concessionaire's Public Wi-Fi Service
- Services provided by third parties that can directly impact on the delivery of the Concessionaire's Public Wi-Fi Service.

Any exceptions to this policy shall be recorded, entered into the risk register and a formal risk assessment carried out.

Objectives

The Objective is to achieve a Best Practice Change Management process with the key benefits of:

- Cost effective Change Management;
- Visibility & analysis of incident rate caused by planned outages;
- Improved customer notification of outages;
- Improved customer satisfaction;
- Improved visibility and management of the Concessionaire's Public Wi-Fi Service.

The format of a Request For Change template (RFC) will be agreed between the Authority and the Concessionaire.

Requirements of the TFL IM Service Desk:

The Concessionaire requires the Authority to nominate Change Authority who will have the authority to agree Request for Changes and Emergency Requests for Change as per the agreed process which will be defined in the Operational Agreement.
The nominated Change Authority will also need to evaluate Requests for Change from TFL IM Service Desk to the Concessionaire Service Desk, prior to submission.
Requests by TFL IM Service Desk for Emergency Planned Changes, should be made direct to the Concessionaire's Service Desk and the Concessionaire's Service Relationship Manager for information.

We expect to agree a reciprocal notification period for changes which will be reasonable to maintain the agreed target SLA for the service.

5.0 Escalation Procedure

The Escalation Matrix will be defined and agreed during the mobilisation phase of the project roll-out

This process can be activated on an Impact / Urgency basis and a SLA failure basis. The Concessionaire's Escalation path is a named process from Duty Manager to Operations Director.

Principle:

Fault Incident escalation process

Escalation will be invoked if the Incident is in jeopardy of not being resolved within the agreed SLA. Escalation will be proactively initiated by either Service Desk should a fault or order fail to meet any of the service standards or there is reason to believe the standards will not be achieved.

Service/Account escalation process

If at any point TFL IM Service Desk or Management team feels that the completion or resolution of an Incident is not progressing to their satisfaction then the issue should be escalated to the Concessionaire's Service Desk Supervisor and the Service & Account Managers.

Should circumstances dictate TFL IM Service Desk may request escalation to expedite an Incident. The Concessionaire's Service Desk Representative will take the escalation and report it to the Service Desk Supervisor who will assume ownership, and agree with TFL IM Service Desk the appropriate course of action.
Updates will be provided to TFL IM Service Desk and the Concessionaire's Service Relationship Manager. The Account Manager will also be advised of the situation.
In exceptional circumstances based on Impact and Urgency, the Authority will be able to skip escalation levels direct to Director Level. Such circumstances will follow the Major Incident process, which will be defined and agreed within the Operating Agreement.

Example Escalation Matrix

Escalation Level	Escalated To		Time Elapsed
	The Concessionaire	The Authority	
1	FMC Team Leader / Service Manager / Account Manager		> 4 hrs
2	FMC Manager & Business Service Relationship Manager		> 6 hrs
3	Service Assure Manager & Head of Service Management		> 8 hrs
4	Director of Customer Service		> 12 hrs

5	Director of Business Operations		> 24 hrs

Requirements of the TFL IM Service Desk:

Agree and populate Escalation matrix for contacts during Traffic Hours and outside of operational hours.

6.0 Disaster Recovery & Business Continuity

The Disaster Recovery plan for the Public Wi-Fi Service will be defined and agreed and documented in the Operational Agreement. Including the agreed definition of a disaster and the relevant disaster scenarios with the agreed course of action and owners detailed. The plan will be owned and managed by the Concessionaire and the implementation of the plan is the responsibility of the Concessionaire.

Principle:

The Concessionaire has DR plans for existing teams and services across our Business. These plans are wholly owned and managed by the Concessionaire and the implementation of such plans is the responsibility of the Concessionaire.

Concessionaire WiFi operational functions are integrated into these existing teams and we expect the WiFi Operational points of contact etc to work continuously in the case of an incident. We will be happy to take the Authority through the detail of this and to agree any impact to them and vice versa.

It is vitally important to the success of the Concessionaire that it can maintain its services with minimal interruption. Business Continuity Management (BCM) ensures that we can continue undertaking our critical activities in the event of a substantial incident.

The aim of this Business Continuity Plan (BCP) is to ensure that we can return to normal service levels within a pre-determined timescale that reflects the needs of our customers.

Purpose

The purpose of a Business Continuity Plan is to outline:

- The BCM objectives
- The roles and responsibilities of staff directly involved in key recovery activities
- Recovery activities
- A summary of information to support recovery actions
- Key tasks to guide staff within to achieve continuity objectives

Scope

The scope of the plan includes:

- The critical activities for the key processes used by the Concessionaire

- All Staff and Contractors who work for the Concessionaire
- Suppliers
- Links with the rest of the Concessionaire's businesses including Crisis Communications links to the Incident Management Process

Objectives

The main objectives of the plan are to:

- Ensure the safety of staff that work within the Concessionaire and as relevant, any staff of TFL, end customers and the public in general.
- Minimise the impact of an incident by recovering to pre determined levels of service.
- Ensuring that sound communication links are maintained during the recovery period.
- Ensure that the Concessionaire works effectively with other Partners and Suppliers during the recovery period.

A copy of the Concessionaire's BCM Policy statement is included in Appendix B.

For the avoidance of doubt, there is no dependency on the Authority for the implementation of the Concessionaire's BCM plans.

Requirements:

The Authority to work with the Concessionaire to formulate a plan based on site priority level and identify solutions to mitigate risk as relevant.

The Authority to confirm that their Service Desk Continuity Plan is in place and share relevant information to the Concessionaire's Service Desk.

7.0 Security breaches, Notification & Handling

The Concessionaire is accredited against the security standard referred to as NGN 224.

NGN224 is the project reference to the Security Procedures, Telecommunication Systems and Services, Issue No: 1.0, July 2009 document released by CESG. NGN224 builds over ISO27001 information security standard and defines more specific clauses for communications services providers.

The focus of CESG is to provide guidance to public sector organisations for security requirements they should ask from communication providers.
As NGN224 is based on ISO27001 it requires the definition, implementation and sustained management of an information security governance framework.

A process will be agreed for the handling of any requests relating to the Service pursuant to Clause 13, (including but not limited to RIPA and data retention) where the Authority upon receipt of a request shall inform the requester that the Authority does not provide the WiFi Service and that the requester must contact the Concessionaire. The Concessionaire will then take responsibility for any resolution.

Principle:

The Network Security Incident Procedure addresses how Resolver Groups Incident Management action their responsibilities when security events / faults occur or weaknesses are identified.

The purpose of this procedure is to document the actions required when a network security incident is identified.

This procedure is integrated with the Network Activate and Operate fault management process. It uses the major components of the Incident management process, supported by the Concessionaire's Remedy System to enable the management of security incidents.

Within the Remedy system Security Incidents are differentiated by completing a specific incident type tickbox. All Security Incidents on Remedy are managed by the Network Incident Management team.

Network Incident Management is a 7x24 team within Activate & Operate. Their role is to provide jeopardy management and communications on high priority incidents. When they are contacted about a Security incident they reveal information on a "need to know" basis to minimise the potential leakage in information that could harm or impact the brand or reputation

A security incident is defined as a single or series of unwanted or unexpected security events that have a significant probability of compromising, or threaten to compromise, the confidentiality, integrity or availability, of the service provided, including the network infrastructure, network management systems, the Concessionaire or customer information.

Security incidents can be related to technical and non technical issues or a combination of both.

In relation to security events the terms confidentiality, integrity and availability, are used as detailed below:

- Confidentiality information related to the service, network infrastructure, network management systems the Concessionaire and customer data is not available or disclosed to unauthorised individuals or entities
- Integrity the accuracy and completeness of the network infrastructure, network management systems, the Concessionaire's and customer information are safeguarded

- Availability the service, network infrastructure, network management systems, the Concessionaire and customer data remain accessible and usable by authorised entities

All incidents relating to confidentiality or fraud issues are raised with internal Group Security.

In the event of the Concessionaire indentifying a security breach which could have a service impacting issue to TFL, the TFL IM Service Desk will be notified following the Major Incident process, detailed in the Operational Agreement.

Requirements:
As TFL IM Service Desk will be managing the TFL Wi-Fi Infrastructure, the Concessionaire's Service Desk will require cooperation with the TFL IM Service Desk to agree, develop and share best practice in managing security incidents.

We will agree the process for identified potential threats and then a major incident procedure to cover actual breaches.

We will identify points of contact for managing any major incidents within our Major Incident service team and Wi-Fi service management team.
Stakeholders, such as the Service Relationship Manager, Head of Service Management, Account Manager, Head of Wi-Fi, and Director of Wireless for the Concessionaire, with the Authority expected to provide the reciprocal stakeholders.
Details of key stakeholders contacts for Major Incidents will be detailed in the Operational Agreement.

In the event of a Major Security Incident, a meeting will be convened at the earliest opportunity to discuss the detail of the incident, agree the relevant action plan including mitigation plans and any public statements required.

We will require the Authority to provide a reciprocal level of transparency to the security of their systems and any threats including details on what actions are being taken to protect the Concessionaire's Public Wi-Fi Service.

8.0 Controlled Shut Down (i.e. when requested by police) & Graceful resumption

In the event that the Authority request the temporary immediate closure of the Concessionaire's Public Wi-Fi Service, a number of options are possible. *Currently waiting on the Technical team to confirm the most graceful way of shutting the service down.*

Requirements:
The Authority will need to provide the Concessionaire with a list of authorised representatives who have the authority to request shut down and restoration of service on behalf of the Authority.

We expect that the best place to shut the service down will be via the WiFi Controllers which are within the control of the Authority. Therefore we will need to agree a process for communication for turning it off and bringing it back. Such process will be documented in the Operational Agreement.

In the event that the Authority is instructed by the Police or Security Services to immediately shut down the Public Wi-Fi Service, TFL IM Service Desk can immediately implement the Shut down without seeking the permission of the Concessionaire's Service Desk.

The Concessionaire's Service Desk would require notification of Shut Down within 15 minutes or as reasonably possible under the specific circumstances in order to activate announcements on our Customer Contact centre.

For partial shut down, such as specific stations and access points, the Concessionaire expects TFL IM Service Desk to notify the Concessionaire's Service Desk as soon as reasonably possible, with 30 minutes in order to activate announcements on our Customer Contact centre.

The various Shut down scenarios and required responses, such as Web Site Landing page information and Customer Contact Centre Announcements will be agreed and documented in the Operational Agreement.

09. Contact Methods

Principle: Both the Authority and the Concessionaire have the same interest in the Public Wi-Fi Service delivering an acceptable level service to the consumer. As such we expect to develop a close working relationship between both Service Desks. We expect the teams to meet to develop a working relationship where issues are resolved for the benefit of the service.

TFL IM Service Desk will be provided with a 24x7x365 free phone number for the Concessionaire's Service Desk and a 4 digit PIN which will clearly identify the Authority as the calling party.

TFL IM Service Desk will also be provided with the direct contact details of the Account Support team, such as the Service Relationship Manager, Account Manager, Project Manager and the agreed Escalation processes. All such details will be documented in the Operational Agreement.

Requirements: The Authority will be required to provide a Service Desk and service management support in order for the Concessionaire's Service Desk to report suspected Incidents on the Concessionaire's Public Wi-Fi Service.

The Authority will be requested to populate a key personnel contact section and Escalation matrix which will be documented in the Operational Agreement.

Our requirements on the Authority

The Authority will be responsible for managing and maintaining the Wi-Fi Infrastructure which will provide internet access to customers of both organisations who use the Authority's network.

The Concessionaire fully recognises the benefits of enabling Wi-Fi across the Authority's network and also recognises the support limitations that providing service in the underground network environment will encounter due to Health & Safely requirements.

The Concessionaire sees a key success measure for both organisations is the end user experience that will be paying for the service. This success will be driven by both organisations working in partnership and sharing best practice and common goals.

Directing customers to the Concessionaire

This will be defined as part of the Product Launch program and product literature to ensure the end customer contacts the Concessionaire and does not raise an issue direct with the Authority.

Training & awareness of the Authorities staff

Whilst the Concessionaire is expecting to manage the customers we are unable to stop them contacting the Authority directly. Therefore the Concessionaire proposes to work with the Authority to put a plan of action in place for example provide 'welcome packs' to the Authority's staff which will provide sufficient awareness of the new service and instructions on what to do if approached by a member of the public with a Wi-Fi query.

The Concessionaire's marketing department will work closely with the Authority when designing and agreeing the content of the Welcome Pack.

Example Reports

The Concessionaire requires Radio Access Network performance statistics to verify that the Concessionaire Public WiFi Service elements are fully meeting the demand captured and transported by the Authority's Infrastructure network.

Typically, the Concessionaire provides a network performance report as part of the monthly performance reporting pack. The report details the performance of the network devices on a site by site basis. This would include such KPI's as:

- Site Availability
- Bandwidth Utilisation
- Latency

As the Authority will be monitoring, maintaining and managing the Wi-Fi Infrastructure, the type of performance reports available will be dependant on the performance tools available to the Authority.

The Concessionaire will provide a monthly performance report based on the number of incidents logged between the TFL IM Service Desk and the Concessionaire's Service Desk.

The report will also include a manually calculated network availability statement relevant to the Concessionaire service's elements including Portal availability.

Example Monthly Performance reports are included in Appendix C

The Revenue Share reports will be provided by the Concessionaire's Account Manager

Appendix A – Example Fault Management Process

Fault Management

2.4.1 Provision of maintenance

Where agreed, each Operator will specify a single contact point for fault communication. This Single Point of Contact (SPOC) - also known as the Fault Reporting Point, (FRP) shall be:

For the Concessionaire:

Virgin Media Service Desk
Phone: [redacted]
E-mail: [redacted]

For the Authority: details of SPOC shall be provided to the Concessionaire within 14 days of the Agreement Commencement Date.

In addition: -

- It is the responsibility of each Operator to ensure that all staff observe the Health & Safety at work Act. All digressions must be reported. This includes access without a current permit to work.
- Procedures covering work with lasers must be observed at all times. It is particularly important to ensure that lasers are powered down *prior* to work commencing.
- All work must be pre–approved with a *current* Permit to Work issued.
- Only qualified staff will work on power systems.
- Operator's standard maintenance procedures must be observed at all times.

2.4.2 Fault Reporting

Initially all faults will be reported verbally via telephone to the SPOC / FRP. Virgin Media Business will generate a unique reference number. This number will be quoted in all verbal or written correspondence related to that fault, and will be used in any subsequent communication whilst progressing the fault through to resolution.

2.4.3 Points of Contact

These are as detailed in paragraph 2.4.1, and Appendix D of this document. It is the responsibility of the document owner to ensure the contact details are updated.

2.4.4 Fault Run-time

To assist both Operators to analyse fault conditions it is important that the same criteria for measurement are used.

2.4.4.1 Fault Start Time

The time the fault is first raised and entered onto the Fault Database by the originating Operator. (When the fault is first detected by either Operator).

2.4.4.2 Fault Restoration Time, (service restoration)

The time when either Operator has notified, or has attempted to notify, the other party of the fault having being fixed.

2.4.4.3 Fault Closure Time

The time when either Operator confirms to the raising Operator's FRP that service has been restored or all attempts to confirm have been unsuccessful and are then abandoned.

2.4.4.4 Access Restrictions

Where access is required but not approved or provided, the clock will be stopped until access is granted. Careful note should be taken of the 'non-accessibility' time so it can be deducted from the overall fault run time.

2.4.5 Information Updates

The party controlling the fault will provide *hourly* updates on the progress of Critical Service Affecting faults unless otherwise agreed between the Operators. (Updates for other fault categories are to be agreed between the respective NMC's where appropriate).

Both Operators may agree to less frequent update periods. This is particularly appropriate with an Out of Hours Fault.

Additionally, either Party may request more frequent updates at any time (via their respective NMC), by quoting the unique fault reference number.

2.4.6 Fault Clearance

The Operator controlling the fault will verbally notify the other Operator *within 30 minutes* that a fault condition has been cleared.

This should follow internal notification from their engineering staff that service has been restored and is available.

If fault clearance cannot be agreed then either party may initiate: -

- Joint Testing
- Escalation process via the contacts detailed in Appendix D

2.4.7 Fault Report Closure

A fault is to be closed, and the clock stopped, only with the agreement of both Operators, (the one exception is per 2.4.4.3 – where contact cannot be made).

Fault closure can result from: -

- A permanent fix,
- A temporary fix, or
- By reconfiguring the route and restoring the service.

In the case of the second and third options both Operators must discuss and agree on a permanent solution. (The most common being a future Planned Work).

The following information is to be verbally agreed and recorded by both parties on their respective fault logging systems when closing faults:

- Names/contact numbers of both representatives at closure
- Service restoration time
- Fault resolution time
- Fault resolution / service restoration actions taken.
- Duration of any period where access was an issue, see section 2.4.4

Appendix B – BCM Policy

Business Continuity Management

Policy Statement

OBJECTIVE

To ensure that Virgin Media's services and assets are safeguarded in a cost effective manner against events or actions which might otherwise materially damage the company or its customers.

Notes:
Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

Assets Include:
Information Assets: *Including databases, data files, system documentation, user and training manuals, operational procedures, archived information etc.*
Software Assets: *including application software, system software, development tools and utilities.*
Physical Assets: *Computer equipment, communications equipment, media.*
Service/Support Assets: *including technical and office buildings, power, air conditionings, heating, lighting, supplies, suppliers etc.*

People: *plans should take account of key staff, whether permanent, temporary, or contract where they are involved in service processes*

Legislation & Standards Include:
BS 25999-1 Business Continuity Management – Part 1 Code of practice
BS 25999-2 Business Continuity Management – Part 2 Specification
BS ISO/IEC 17799:2005
BS ISO/IEC 27001:2005 (BS7799-2:2005)
Civil Contingencies Act 2004
Data Protection Act 1998
Health & Safety at Work Act 1974

Inclusive of any relevant company policies and procedures in place.

NB. *A supporting BCM Framework, standards, guidelines, and procedures are being developed to underpin this policy statement.*

1.1 POLICY

- Business Continuity Management (BCM) is concerned with managing risks to ensure that at all times Virgin Media can continue operating to at least a pre-determined level.
- The Security & Resilience Group has approved the BCM framework.
- Governance of the framework will be provided through:
  - ❖ Security & Resilience Group, led by the CTIO Managing Director and coordinated through the Group Security function. This Group will meet and report bi-monthly
  - ❖ The BCM framework will be implemented within divisional Service Areas, supported by divisional representatives and overseen by Group Security
  - ❖ Business Continuity Strategies will be developed at divisional levels across Virgin Media, ensuring a consistent corporate response, and achieving economies of scale
  - ❖ A robust programme of audit, testing and maintenance, in accordance with BS25999-1 & BS25999-2, will be integrated into Business Continuity Plan development at divisional level
- It is the policy of Virgin Media to ensure that:
  - ❖ All Business Units carry out Business Impact Analysis and subsequent Risk Assessment.
  - ❖ Relevant and appropriate Business Continuity Plans (BCPs) exist for all Business Units, and these will be supported by Divisional and site-specific procedures. These plans should be consistent with the corporate BCM framework
  - ❖ A process for training, education and awareness to support divisional BCPs will be implemented, and be consistent with the BCM framework
  - ❖ A continuous process of low level risk management will be implemented to identify and reduce risks and limit the consequences of damaging incidents should they occur *(Note: this will be complimentary to existing measures already coordinated through Virgin Media's Group Risk department)*
- The Business Continuity Manager has **direct responsibility** for maintaining the BCM Framework and providing advice and guidance on its implementation.
- All divisional Managing Directors are **directly responsible** for implementing the BCM Framework within their business areas.
- It is the responsibility of **each** employee to assist in the implementation of this policy within his or her area of work.

Appendix C – Example Reports

Example LU WiFi
Portal SLA Performan

CP6 1
7_WiFiDashboard.pdf

Example Report - Impressions and Clicks Detail

LUL/Virgin Impressions and Clicks Detail Report for the period from 4/12/2011 to 4/12/2011

Location	Displayed/Clicked Item Name	Impressions	Clicks	CT Rate
Online Underground Homepage	Underground Map widget	177,397	25,031	14.11%
Online Underground Homepage	Service Status widget	177,397	13,421	7.57%
Online Underground Homepage	Carousel - Olympics	177,397	5,600	3.16%
Online Underground Homepage	Carousel - News	177,397	4,860	2.74%
Online Underground Homepage	Carousel - Weather	177,397	3,078	1.74%
Online Underground Homepage	Carousel - Sport	153,123	2,672	1.75%
Online Underground Homepage	Carousel - Entertainment	142,312	2,218	1.56%
Online Underground Homepage	Carousel - Stock Markets	121,231	1,834	1.51%
Online Underground Homepage	Carousel - TV Listings	90,241	1,778	1.97%
Online Underground Homepage	Carousel - Cinema	70,800	1,206	1.70%
Online Underground Homepage	Carousel - What's On	67,001	1,204	1.80%
Online Underground Homepage	Carousel - London Underground	65,983	1,168	1.77%
Online Underground Homepage	Get Internet Access button	177,397	1,062	0.60%
Online Underground Homepage	Twitter updates	177,397	7,023	3.96%
Online Underground Homepage	Facebook updates	177,397	11,021	6.21%
Online Underground Homepage	Menu	177,397	15,231	8.59%
Online Underground Homepage	Menu item - Get Internet Access	15,231	1,312	8.61%
Online Underground Homepage	Menu item - FAQs	15,231	701	4.60%
Online Underground Homepage	Menu item - Games	15,231	503	3.30%
Online Underground Homepage	Menu item - Quick Survey	15,231	401	2.63%
Online Underground Homepage	Menu item - Service Status	15,231	2,101	13.79%
Online Underground Homepage	Menu item - Journey Planner	15,231	241	1.58%
Online Underground Homepage	Menu item - Weather	15,231	111	0.73%
Online Underground Homepage	Menu item - Stock Market News	15,231	131	0.86%
Online Underground Homepage	Menu item - TV Listings	15,231	93	0.61%
Online Underground Homepage	Menu item - What's On in London	15,231	801	5.26%
Online Underground Homepage	Menu item - Competitions	15,231	202	1.33%
Top 50 Total			**105,004**	

Impressions represent the number of times a particular asset has been seen by all customers.

E.g. if an item is located on the page once, then the impression count will be equal to the pageview count.

Clicks represent the number of times a particular asset has been clicked on by all customers.

CT Rate represents the "click-through rate" of each asset, and is calculated by dividing the asset impressions by the asset clicks.

Example Report - Pay As You Go Revenue

Package	Rate	Subscriber numbers	Gross Revenue	Cost of Sales	Total Net Revenue	London Underground Revenue share [redacted]
1[redacted]	[redacted]					
[redacted]	[redacted]					
[redacted]	[redacted]					
[redacted]	[redacted]					
Total						

Advertising Revenues

Campaign	CPM	Page impressions	Gross Revenue	Cost of Sales	Total Net Revenue	London Underground Revenue share [redacted]
Campaign #1						
Campaign #2						
Campaign #3						
Campaign #'n'						

Wholesale Partner Revenue

		Total Net Revenue	London Underground Revenue share [redacted]
Wholesale partner 1			
Wholesale partner 2			
Wholesale partner 3			
Wholesale partner 'n'			

Example Report - Service Management
Customer Meeting Report

Customer:					
SM :		**Date:**		**Venue:**	
Meeting Type:	**PLANNED REVIEW** COURTESY VISIT URGENT ISSUE				
Next Meeting Date:				**Venue:**	

Attendees	Responsibility	Company

Apologies		

Start Time:		**Finish Time:**	

Example Report - Service Management
Customer Meeting Report

Item	Issue	Resolution / Actions	Who	Status	Date Closed
01					
02					
03					
04					
05					
06					

Appendix D – Escalation Points of Contact

Concessionaire Contact Details

Job Title / Name	Contact Details	E-Mail
DINMC	[redacted]	[redacted]k
Manager DINMC 1st Line Mike Fellows	[redacted]	[redacted]
Incident Management	[redacted]	[redacted]
Head of Voice / Head of Data & Internet Kevin Hallissey	[redacted]	[redacted]

Concessionaire Escalation Details

Escalation Level	Job Title / Name	Contact Details	E-Mail
1	DINMC Shift Leader	[redacted]	[redacted]
2	Manager DINMC 1st Line Mike Fellows	[redacted]	[redacted]
2	Incident Management **Note 1**	[redacted]	[redacted]
3	Head of Voice / Head of Data & Internet Kevin Hallissey	[redacted]	[redacted]
4	Executive Director, Operations Steven Hobbs	[redacted]	[redacted]
5	Chief Customer & Networks Officer Paul Buttery	[redacted]	[redacted]

Note 1: Incident Management escalation point is to be utilised in the following circumstances:

- Incident Management will only be involved in CSO or MSO faults and some selected P1's that are deemed to be high customer impacting. (Note TfL v Virgin Media fault severity/priorities are to be agreed)
- DINMC request Incident Management assistance in escalating the fault with TfL. In this instance Incident Management will assist with escalating the fault within TfL organisation.
- TfL may request Incident Management assistance to escalate a fault within the VM DINMC in instances where TfL is unable to get a timely response from the DINMC level 1 or 2 escalation points.

Note 2:

- DINMC and Incident Management is due to relocate from their current locations at Crawley Court to VM's Langley office. This move is to take place on 16th April at 07:00. Following this move VM will issue a new contact phone number for the DINMC.
- A call tree option will also be setup for the LU WiFi desk within the DINMC.
- E-mail addresses will remain as shown.

The Authority's contact details and details of its escalation process shall be provided to the Concessionaire within 14 days of the Agreement Commencement Date.