Business Operations Agreement

Schedule 2

General Statement of Requirements

Service Operations Department
Transport for London
4th Floor, Palestra
197 Blackfriars Road
Southwark London SE1 8NJL

Table of Contents

APPENDICES

Appendix 03 Volumetrics

Appendix 09 IIP Standard

Appendix 10 Information Governance

Appendix 11 Data Retention

Appendix 13 Interface Catalogue

Appendix 16 Handling Evidence

Appendix 17 Elise CUG Code of Connections

Appendix 18 Secure Handling and Classification of Information

STATEMENT OF REQUIREMENTS

This document, along with its appendices, is part of schedule 2 (Statement of Requirements) of the Business Operations Agreement. Schedule 2 provides the requirements for the Business Operations, MIS, Finance, Interoperability, VoSI and General Service Elements.

This document should be read in conjunction with other component documents of the Agreement as these play an integral part in understanding the requirements set out in this document.

Definitions of terms used in this document are contained in schedule 1 (Definitions).

In meeting the Requirements set out in this Schedule 2: Statement of Requirements (Business Operations) the Service Provider shall at all times ensure that the Requirements are delivered in accordance with Clause 4 *(TfL Objectives*) of this Agreement.

The structure and layout of this document is ordered into sections. Each section has a heading with an introductory statement. This is followed by sub-headings containing requirements. Each requirement has two rows containing the following information (see example of layout of Statement of Requirements):

- Requirement number;
- Mandatory; and
- Requirement detail.

Example of Layout of Statement of Requirements

Z1.1.1		Mandatory
Individual requirements are located from here onwards.		

The Requirement number indicates the number of the individual Requirement and is made up of one (1) letter and three (3) numbers. The letter indicates the Statement of Requirements to which this requirement relates to (e.g. Z = General). The first number relates to the section number, the second number relates to the sub-section and the third number relates to the Requirement number within that sub-section.
The Service Provider shall ensure that a mandatory Requirement is met.

Where a new requirement has been created it may have a letter added at the end of the requirement number, for example B 4.1.1b. The letter has been added to the requirement to ensure correct sequencing, it does not not indicate a sub-requirement.

1. GENERAL
This section covers the generic requirements applicable to the Service Provider.
1.1 General Requirements

Z.1.1.1		Mandatory
The Service Provider shall comply with all standards, policies, processes, procedures, and measures requested by TfL during the term of this Agreement and in accordance with Schedule 9: Change Control Request Procedure.		

Z.1.1.2		Mandatory
The Service Provider shall Maintain the Compliance Matrix throughout the term of this Agreement.		

Z.1.1.3		Mandatory
The Service Provider shall complete and Maintain the IPR Summary Table in accordance with Volume 1, Appendix 10 – IPR Summary Table throughout the term of this Agreement.		

APPLICABLE FROM THE ULEX OPERATIONAL COMMENCEMENT DATE		
Z.1.1.4		Mandatory
The Service Provider shall manage the Cloud Services in a manner that is consistent with Good Industry Practice, regularly monitoring and taking reasonable steps in considering and where appropriate implementing any recommendations made by Azure Advisor, the objective being to minimise the cost to TfL within the context of the Service Provider's wider capacity management responsibilities. Without limiting the foregoing, the Service Provider shall disclose to TfL all Advisor Recommendations, and the Parties shall meet to discuss such Advisor Recommendations on a monthly basis during the first 6 months from the ULEX Operational Commencement Date, and on a quarterly basis thereafter. Where the Service Provider (acting reasonably) determines that it would not be appropriate, in the context of its wider capacity management responsibilities, to implement the Advisor Recommendations, then the Service Provider shall be under no obligation do so, but where this is the case the Service Provider shall provide to TfL an explanation of its reasons for not implementing such recommendations.		

2. STANDARDS, WORKING PRACTICES & PRINCIPLES

This section covers those requirements relating to the standards, working practices and principles to which the Service Provider shall adhere in providing the Services.

2.1 Standards, Working Practices & Principles

Z.2.1.1		Mandatory
The Service Provider shall in the performance of its obligations under this Agreement, comply with all obligations in relation to Privacy Legislation as may be amended or superseded by equivalent legislation from time to time in accordance with Clause 49.		

Z.2.1.2		Mandatory
The Service Provider shall in the performance of its obligations under this Agreement, comply with all obligations in relation to the Freedom of Information (FOI) Legislation as may be amended or superseded by equivalent legislation from time to time in accordance with Clause 49.		

Z.2.1.3		Mandatory
The Service Provider shall in the performance of its obligations under this Agreement comply with all obligations in relation to the Computer Misuse Act 1990 as may be amended or superseded by equivalent legislation from time to time in accordance with Clause 49.		

Z.2.1.4		Mandatory
The Service Provider shall in the performance of its obligations under this Agreement comply with all obligations in relation to the Environmental Information Regulations 2004 as may be amended or superseded by equivalent legislation from time to time in accordance with Clause 49.		

Z.2.1.5		Mandatory

The Service Provider shall develop and comply with processes for Configuration Management in accordance with this Statement of Requirements and shall submit such processes to TfL for Assurance before the Operational Commencement Date and operate them for the Term of this Agreement.

Z.2.1.6		Mandatory
The Service Provider shall develop and comply with processes for Incident Management and shall submit such processes to TfL for Assurance in accordance with this Statement of Requirements and Schedule 5:Service Level Agreement before the Operational Commencement Date and operate for the Term of this Agreement.		

Z.2.1.7		Mandatory
The Service Provider shall develop and comply with processes for Release Management and shall submit such processes to TfL for Assurance in accordance with this Statement of Requirements before the Operational Commencement Date and operate for the Term of this Agreement.		

Z.2.1.8		Mandatory
The Service Provider shall develop and comply with processes for Change Management and shall submit such processes to TfL for Assurance in accordance with this Statement of Requirements and Schedule 9: Change Control Procedures before the Operational Commencement Date and operate for the Term of this Agreement.		

Z.2.1.9		Mandatory
The Service Provider shall comply with all applicable Laws, regulations and standards in accordance with this Agreement, during the Term.		

Z.2.1.10		Mandatory

The Service Provider shall adhere to the standards and working practices set out in Table 1 below, as such standards may be amended or superseded by equivalent standards from time to time.

Table 1– Standards and Working Practices

ISO/IEC 27001:2005 and ISO/IEC 27002:2005	for Information Security Management
BS ISO/IEC 6592	Guidelines for the documentation of computer-based application Systems
BS EN ISO 9000-3	Guidelines for the application of ISO 9001:2000 to the development, supply, installation and maintenance of computer software
BS EN 60950	Specification for safety of information technology equipment, including electrical business equipment
BS EN 60529	Specification for degrees of protection provided by enclosures (IP codes)
BS EN 60073	Basic and safety principles for man-machine interface, marking and identification. Coding principles for indication devices and actuators

Z.2.1.11		Mandatory
The Service Provider shall develop and comply with a framework such as ITIL or ISO 20000 to undertake Service Management and shall submit such framework to TfL for Assurance within one (1) month of the Effective Date.		

Z.2.1.12		Mandatory
The Service Provider shall operate so as to give a seamless TfL customer experience when interacting with Customers (subject always to this Agreement).		

Z.2.1.13		Mandatory
The Service Provider shall ensure that the TfL corporate branding provided by TfL from time to time is used exclusively at all times across all Communication.		

Z.2.1.14		Mandatory
The Service Provider shall ensure that at no time shall it use its own name, branding and corporate logo (or the name, branding and logo of any other entity besides that of TfL) in any Communications.		

3. INFORMATION GOVERNANCE

This section covers the generic requirements applicable to the Service Provider in relation to Information Governance. These requirements include the following:

- Generic requirements;
- Information Access Requests;
- Subject Access Request(s);
- Contractors;
- Complaints;
- Reporting of breaches of Privacy Legislation; and
- Data Protection audit.

3.1 Information Governance

Z.3.1.1		Mandatory
The Service Provider shall ensure that the Service System(s) provides the functionality to enable and require a Customer to opt-in or opt-out of direct marketing from TfL and any other Third Party.		

3.2 Freedom of Information Requests

Z.3.2.1		Mandatory
The Service Provider shall submit to TfL for Approval prior to the Operational Commencement Date, and when Approved comply with, a process on how to respond to Freedom of Information Requests such proposed process to include (but not limited to) a format for presenting to the Customer any relevant Data surrounding the Freedom of Information Request (e.g. Data table, graphical representation, copy of Document etc).		

Z.3.2.2		Mandatory

The Service Provider shall submit to TfL for Approval, and when Approved, comply with, a procedure to deal with FOI requests where the Customer is unable to provide written correspondence, for the avoidance of doubt written correspondence shall include but not be limited to email.

3.3 Data Retention

Z.3.3.1		Mandatory
The Service Provider shall comply with all TfL's specific requirements relating to retention periods for all Data as specified in Appendix 11: Data Retention. Where no period has been specified, the Data will be retained for as long as is required for the purpose for which it was collected, and no longer in accordance with Appendix 11: Data Retention.		

Z.3.3.2		Mandatory
The Service Provider shall securely delete all Data at the expiry of its retention period, in accordance with Appendix 11: Data Retention.		

Z.3.3.3		Mandatory
The Service Provider shall ensure that all Data deleted at the expiry of its retention period cannot be accessed by anyone. Data held on paper shall be securely shredded and Data held electronically shall be deleted using tested deletion scripts in accordance with Schedule 14: Security and this Statement of Requirements.		

Z.3.3.4		Mandatory
The Service Provider shall use industry standard disk-wipe software and other mechanisms in accordance with Schedule 34: TfL Policies ("TfL's Secure Erasure and Disposal Policy – IM-S-PO-035") to make unusable all media that are no longer operational. This includes optical disks, floppy disks, hard disk drives, solid state storage, paper and tapes. This process of securely erasing media shall be documented and tested, and shall include the production of certificates of destruction as required by TfL.		

Z.3.3.5		Mandatory
The Service Provider shall ensure that the Service System(s) provide the functionality to protect Data from automatic deletion in the event that it is required for further reference.		

Z.3.3.6		Mandatory
The Service Provider shall ensure that the Service System(s) provide the functionality to remove the protection on data so that the data can be destroyed in accordance with Appendix 11: Data Retention.		

3.4 Data Protection

Z.3.4.1		Mandatory
The Service Provider shall submit to TfL for Approval, and when Approved, comply with a mechanism for the validation of Data at the point such data is entered into the Service System(s).		

Z.3.4.2		Mandatory
The Service Provider shall ensure that all Data Stores comply with this Statement of Requirements, and Appendix 11: Data Retention.		

Z.3.4.3		Mandatory
The Service Provider shall collect and process Personal Data only in accordance with the instructions and directions given by TfL and in accordance with Privacy Legislation.		

Z.3.4.4		Mandatory
The Service Provider shall store and Process all Personal Data, with the exception of DVLA Data, within the European Economic Area (EEA). The storing and Processing of Personal Data outside of the EEA is prohibited. For avoidance of doubt, Processing shall include (but is not limited to) the ability to read the data.		

Z 3.4.4b		Mandatory
The Service Provider shall not store or access DVLA Data outside the United Kingdom save to the extent agreed by the Parties in accordance with the Change Control Request Procedure (such procedure to involve associated discussions with the DVLA).		

Z.3.4.5		Mandatory
The Service Provider shall protect all Personal Data against unauthorised and unlawful processing, accidental loss, alteration, destruction and damage in accordance with Privacy Legislation.		

Z.3.4.6		Mandatory
The Service Provider shall use a Privacy Notice in the format set out in Appendix 10: Information Governance		

Z.3.4.7		Mandatory
The Service Provider shall ensure that the Privacy Notice is updated upon request by TfL within five (5) days of such request at no cost to TfL.		

Z.3.4.8		Mandatory
The Service Provider shall ensure that the Service System(s) shall issue a Privacy Notice to any Customer on request by the Customer.		

Z.3.4.9		Mandatory
The Service Provider shall develop and comply with a mechanism for Customer identification checks before any Data amendments are carried out and shall submit such a mechanism to TfL for Assurance.		

Z.3.4.10		Mandatory
The Service Provider shall ensure that where the Services have to revert to manual workaround processes, that adequate measures and controls are in place to protect the		

data against misuse and loss in accordance with Privacy Legislation and PCI DSS regulations.

Z.3.4.11		Mandatory
The Service Provider shall immediately escalate all complaints relating to infringements of Privacy Legislation, civil liberties, equality and human rights to TfL in accordance with the timescales in Schedule 5: Service Level Agreement.		

Z.3.4.12		Mandatory
The Service Provider shall immediately escalate and report all complaints relating to unauthorised and unlawful processing of, accidental loss of, alteration, destruction and damage to Personal Data to TfL in accordance with Schedule 14: Security and this Statement of Requirements.		

Z.3.4.13		Mandatory
The Service Provider shall develop and comply with processes to enable controls to be placed on postal activities to guarantee receipts are processed daily and are not misplaced and misallocated and shall submit such processes to TfL for Assurance prior to the Operational Commencement Date.		

Z.3.4.14		Mandatory
The Service Provider shall provide TfL with certificates of destruction when Data is deleted.		

Z.3.4.15		Mandatory
The Service Provider shall handle any data, including Personal Data, according to the classification given to it by TfL under the "TfL Standard – Information Security Classification" as set out in Appendix 11: Data Retention		

Z.3.4.16		Mandatory

The Service Provider shall notify TfL within five (5) days of all changes to all processes and activities (including locations where they may be undertaken) that will require TfL to update its Notification on the ICO Register of Data Controllers.

Z.3.4.17		Mandatory
The Service Provider shall ensure all VRM(s) are treated as Personal Data		

Z.3.4.18		Mandatory
The Service Provider shall ensure that controls are in place to prevent the copying, reproduction and removal of Data in accordance with Schedule 14 (Security).		

3.5 Data Protection Audit

Z.3.5.1		Mandatory
The Service Provider shall submit to TfL for Approval, and when Approved, comply with, a Data Protection audit plan. The plan shall include: • timescales for preparation and conduct of the annual audit; • the audit strategy and planned outputs; and • details of the independent Third Party undertaking the audit.		

Z.3.5.2		Mandatory
The Service Provider shall comply with the Data Protection Audit Plan.		

Z.3.5.3		Mandatory
The Service Provider shall ensure that a comprehensive Data Protection audit is carried out by an independent Third Party at no cost to TfL. Details of the proposed Third Party must be submitted to TfL for Approval prior to the audit being carried out.		

Z.3.5.4		Mandatory

The Service Provider shall undertake a Data Protection audit every twelve (12) months (or such other frequency as TfL may require) and report the findings to TfL.

Z.3.5.5		Mandatory
The Service Provider shall implement any recommendations from any Data Protection audits within timescales set by TfL.		

3.6 Reporting of Data Protection Breaches

Z.3.6.1		Mandatory
The Service Provider shall report all breaches of Privacy Legislation and all other data security incidents within the period specified in Schedule 5: Service Level Agreement and the Incident Management process.		

3.7 Evidence Store

Z.3.7.1		Mandatory
The Service Provider shall ensure that the Evidence Store complies with Appendix 16: Handling Evidence, specifically: • Section 4 “EVIDENCE COLLECTION AND PROTECTION”; • Section 5 “OFFENCE VIEWING AND KEEPER ENQUIRIES”; and • Section 6 “IMAGE STORAGE AND ARCHIVING”, within the Centre for Applied Science and Technology for handling Evidence.		

Z.3.7.2		Mandatory
The Service Provider shall ensure that DVLA Data is handled in accordance with Appendix 17: Elise CUG Code of Connections as may be amended or superseded from time to time.		

Z.3.7.3		Mandatory
The Service Provider shall ensure that the Data within the Evidence Store is treated as “RESTRICTED”, from an integrity perspective, as defined under the UK Government Protective Marking Scheme (GPMS).		

Z.3.7.4		Mandatory
The Service Provider shall develop and comply with processes that ensure that the transmission of Evidential Records over a public network is done securely in accordance		

with security measures equivalent to those used by major financial institutions for the protection of financial data and shall submit such processes to TfL for Assurance.

Z.3.7.5		Mandatory
The Service Provider shall allow Authorised Users to access and retrieve Evidential Records from the Evidence Store.		

Z.3.7.6		Mandatory
The Service Provider shall ensure that the Evidence Store complies with TfL's security requirements as specified in Schedule 14: Security.		

Z.3.7.7		Mandatory
The Service Provider shall ensure that all access to the Evidence Store is recorded and stored for audit purposes including, without limitation, who accessed it and the date and time that it was accessed.		

3.8 Subject Access Requests

Z.3.8.1		Mandatory
The Service Provider shall submit to TfL for Approval, and when Approved, comply with, a procedure for processing SARs in accordance with Privacy Legislation.		

Z.3.8.2		Mandatory
The Service Provider shall ensure that its Service System(s) are capable of processing, retrieval and printing of SAR information sourced from the Service System(s).		

Z.3.8.3		Mandatory
The Service Provider shall ensure that call recordings can be to be transferred and transmitted to Customers by electronic media as they may form part of a Subject Access Request.		

Z.3.8.4		Mandatory
Where the Service Provider is required to supply information to TfL and any Other Service Provider to enable them to respond to a SAR, the Service Provider shall supply the information required within such time and in such form as reasonably requested by TfL or the Other Service Provider. Where no period of time is specified in the request, the Service Provider shall supply the Information within ten (10) Working Days from the date the request is made to the Service Provider (unless a longer period is specified in advance by TfL).		

Z.3.8.5		Mandatory
The Service Provider shall ensure that a SAR response can be given to a Customer in either hard copy and electronic format if requested to do so by either the Customer or TfL.		

4. SECURITY
This section covers those requirements relating to Security including the Security Policy. This section should be read in conjunction with Schedule 14: Security.

4.1 Access to Systems and Data

Z.4.1.1		Mandatory
The Service Provider shall ensure that Authorised User(s) have the ability to amend Customer Data held on the Service System(s).		

Z.4.1.1b		Mandatory
The Service Provider shall ensure that all Operational User access is limited to the smallest subset of records containing Personal Data appropriate to the activity being carried out.		

Z.4.1.2		Mandatory
The Service Provider shall ensure that the Service System(s) presents all Users with a message reminding them of their obligations to protect Personal Data and that “misuse of the system is an offence under the Computer Misuse Act 1990 and Data Protection Legislation.		

Z.4.1.3		Mandatory
The Service Provider shall ensure that all measures necessary to comply with Privacy Legislation are in place to control access to Personal Data by the Service Provider’s Personnel in accordance with Clause 49.		

Z.4.1.4		Mandatory
The Service Provider shall implement a system to manage access rights to Service System(s) (the "Access and Identity Management Solution").		

Z.4.1.5		Mandatory

The Service Provider shall ensure that the Access and Identity Management Solution electronically receives access right requests from the following sources:

- Change Control Requests;
- Service Requests;
- the Service Providers human resources department;
- TfL's human resources department; and
- Other authorised methods as required by TfL.

Z.4.1.6		Mandatory
The Service Provider shall ensure that the Access and Identity Management Solution verifies that the requestor has a legitimate reason for accessing the requested Service System(s).		

Z.4.1.7		Mandatory
The Service Provider shall ensure that the Access and Identity Management Solution identifies any potential conflicts that may arise in relation to access by any User (for example, the Service Provider shall ensure that a person cannot submit and authorise their own expenses).		

Z.4.1.8		Mandatory
The Service Provider shall ensure that the Access and Identity Management Solution has the functionality to define and amend access rights by role. The Service Provider shall submit to TfL for Approval its proposed access rights by role and, when Approved, implement such access rights by role.		

Z.4.1.9		Mandatory
The Service Provider shall ensure that the identity of Users is authenticated before using any Service System(s) and Services.		

Z.4.1.10		Mandatory
The Service Provider shall ensure that the identity of the Service Provider's Personnel and their location is authenticated before using any Service System(s) and Services.		

Z.4.1.11		Mandatory
The Service Provider shall ensure that TfL Personnel are allocated access permissions to the Service Systems as provided by TfL.		

Z.4.1.12		Mandatory
The Service Provider shall ensure that TfL Users have access to the Service System(s) from any location including, but not limited to, TfL's offices.		

Z.4.1.13		Mandatory
The Service Provider shall ensure that where there is remote access the location of the Operational User and Operational User credentials shall be logged in the Access and Identity Management Solution for audit control.		

Z 4.1.13b		Mandatory

The Service Provider shall log and authenticate the geographic location of the device used by each Operational User logging on to the Service System(s).

The following Matrix gives the location based access control requirements for compliance with Data Protection Legislation and DVLA requirements for handling DVLA Data:

Non-DVLA Data Privileged Employee from:

- Any Location: Deny Access

DVLA Data Privileged Employee from:

- Operational Premises and TfL offices with logged and authenticated geographic location in the UK: Allow Access
- Operational Premises with logged and authenticated geographic location outside of the UK: Deny Access save to the extent agreed by the Parties in accordance with the Change Control Request Procedure (such procedure to involve associated discussions with the DVLA)
- Remote location with logged and authenticated geographic location:

  1. Allow Access if the IP address is located in the UK and is not a known spoofed address.

  2. Deny Access if the IP address is located in the UK and is a known spoofed address.
- Remote location with logged and authenticated geographic location: Deny Access if the address is, or appears to not be in the UK save to the extent agreed by the Parties in accordance with the Change Control Request Procedure (such procedure to involve associated discussions with the DVLA).
- Remote Location without logged and authenticated geographic location: Deny Access

Default:

Operational Premises: Deny Access

Remote location: Deny Access

Non-Personal Data Privileged Employee from:

- Any Location: Deny Access

Personal Data (except DVLA Data) Privileged Employee from:

- Operational Premises and TfL offices with logged and authenticated geographic location in the EEA: Allow Access

- Operational Premises with logged and authenticated geographic location outside of the EEA: Deny Access
- Remote location with logged and authenticated geographic location:
  1. Allow Access if the IP address is located in the EEA and is not a known spoofed address.
  2. Deny Access if the IP address is located in the EEA and is a known spoofed address.
- Remote location with logged and authenticated geographic location: Deny Access if the address is, or appears to not be in the EEA.
- Remote location without logged and authenticated geographic location: Deny Access

Default:
Operational Premises: Deny Access
Remote Location: Deny Access

Z.4.1.14		Mandatory
The Service Provider shall ensure that where remote access attempts are made the location of the User and User credentials are logged and auditable in real time in the Access and Identity Management Solution.		

Z.4.1.15		Mandatory
The Service Provider shall ensure that where a User accesses the Service System(s) remotely for the purposes for Service Management, that User shall not have access to Personal Data.		

Z.4.1.16		Mandatory
The Service Provider shall ensure that remote access is prevented for all operational functions other than Service Management carried out by Service Provider Personnel unless otherwise authorised by TfL.		

Z.4.1.17		Mandatory
The Service Provider shall ensure that credentials used to authenticate Users are held securely within the Service System(s) and that the Service System(s) prevents unauthorised access and retrieval of such credentials.		

Z.4.1.18		Mandatory
The Service Provider shall ensure that the Access and Identity Management Solution stores sufficient information to enable Users to be uniquely identified.		

Z.4.1.19		Mandatory
The Service Provider shall ensure that the Access and Identity Management Solution stores information to link a TfL User to a TfL ID where one exists.		

Z.4.1.20		Mandatory
The Service Provider shall ensure that access to and use of all Service System(s) is subject to appropriate authorisation for access controls in accordance with ISO 27001/2 as such standards may be amended, and/or superseded from time to time.		

Z.4.1.21		Mandatory
The Service Provider shall develop and comply with policies for maintaining the security of all passwords and shall submit such policies to TfL for Assurance.		

Z.4.1.22		Mandatory
The Service Provider shall develop and comply with a User Access Control Policy which complies with ISO27001, whereby access to data is strictly limited to specific roles based on a business need for that role to have access and shall submit such policy to TfL for Assurance. Limits on access shall include but not be limited to: • read access to a specific subset of the Data; • write access on a specific subset of the Data; and		

• changes to specific configuration, Parameters and Reference Data.

Z.4.1.23		Mandatory
The Service Provider shall grant each User the minimum access permissions required for that User to perform their job role. These access permissions shall be reviewed annually by the Service Provider. Proposed amendments to access permissions must be submitted to TfL for Assurance prior to being implemented		

Z.4.1.24		Mandatory
The Service Provider shall ensure that access permissions are allocated and limited to the Service Provider's Personnel and the Service Provider for access to the Service Systems.		

Z.4.1.25		Mandatory
The Service Provider shall immediately disable a User's logon and access rights when a User ceases to be a member of the Service Provider's Personnel, or a User ceases to work on delivering or operating the Service System(s).		

Z.4.1.26		Mandatory
The Service Provider shall immediately, upon notification from TfL, disable a User's logon and access rights when a User ceases to be a member of TfL.		

Z.4.1.27		Mandatory
The Service Provider shall ensure that Service Provider Personnel's internet access is limited to the Approved list of internet sites. The Service Provider shall submit to TfL for Approval, and when Approved, comply with, a list of internet sites accessible by Service Provider Personnel.		

Z.4.1.28		Mandatory

The Service Provider shall ensure that TfL Personnel have unlimited access to the internet from the Service Provider Premises via an independent network to the Contact Centre Services.

Z.4.1.29		Mandatory
The Service Provider shall submit to TfL for Approval, and when Approved, comply withal mechanism for Customer identification checks before any amendments to that Customer's Data are carried out.		

Z.4.1.30		Mandatory
The Service Provider shall ensure all Approved policies for maintaining security of passwords are enforced.		

4.2 Service Systems - Anti-Virus

Z.4.2.1		Mandatory
The Service Provider shall submit to TfL for Approval, and when Approved, comply with processes and procedures to protect the Services System(s) from Viruses, spyware and other potentially destructive devices.		

Z.4.2.2		Mandatory
The Service Provider shall manage the impact of attacks by Viruses, spyware and other potentially destructive Software in accordance with the Approved Incident Management Process.		

Z.4.2.3		Mandatory
The Service Provider shall develop and comply with a 'security patch processing policy' setting out procedures for maintaining the latest versions of leading industry protection Software to address risks of Virus and unauthorised System access and shall submit such a policy to TfL for Assurance.		

Z.4.2.4		Mandatory
The Service Provider shall ensure that security related Software updates are implemented on at least a daily basis to ensure the maximum possible security protection of the Service System(s) and related Software.		

Z.4.2.5		Mandatory
Not Used		

Z.4.2.6		Mandatory
The Service Provider shall 'pro-actively' maintain protection against Viruses, spyware and other potentially destructive devices, including the continued identification and protection against new threats, at no additional cost to TfL.		

4.3 Audit

Z.4.3.1		Mandatory
The Service Provider shall allow TfL Personnel to monitor the Service Provider's compliance and obligations under this Agreement without hindrance. This shall include allowing Authorised TfL Personnel to enter the Premises at any time in order to inspect the operation, maintenance and Equipment used in the provision of the Services.		

Z.4.3.2		Mandatory
The Service Provider shall put in place Data management procedures to ensure that Data is periodically assessed for deletion in accordance with Appendix 11: Data Retention.		

Z.4.3.3		Mandatory
The Service Provider shall maintain sufficient records of Data deletions, as defined by TfL from time to time, to provide a full audit trail to meet the requirements of (but not limited to):		

- the Service System(s) audit;
- TfL's external audit;
- audit by TfL and TfL's internal auditors;
- TfL's management reporting and contract monitoring requirements; and
- Privacy Legislation.

Z.4.3.4		Mandatory
TfL may carry out audits of the Service Provider's quality management systems (including Quality Plans and any quality manuals and procedures) at agreed times in accordance with Schedule 14: Security. The Service Provider shall develop and comply with auditing procedures for audits of the quality management systems and shall submit such procedures to TfL for Assurance.		

Z.4.3.5		Mandatory
TfL may audit the Service Provider's Service System(s) design and operational capability together with, but not limited to, all associated Documentation.		

Z.4.3.6		Mandatory
The Service Provider shall upon request from TfL, allow TfL full access to conduct an audit in accordance with Clause 36: Audit and Inspection. Areas that may be audited will include, without limitation: • the method of report production and any Data transformations; • queries and conditions used for Data extraction from Service System(s); • reconciliation of source to target Data; and • the transfer of Data between Service System(s).		

Z.4.3.7		Mandatory

The Service Provider shall provide full co-operation for any audit including access to all relevant Documentation and Personnel.

Z.4.3.8		Mandatory
The Service Provider shall develop and comply with an audit methodology for monitoring and controlling all business processes and hand-offs to each business function and shall submit such audit methodology to TfL for Assurance.		

Z.4.3.9		Mandatory
The Service Provider shall allow the process used for monitoring and controlling audit(s) to be subject to review by TfL from time to time throughout the term of the Agreement.		

Z.4.3.10		Mandatory
The Service Provider shall develop and comply with an Audit Schedule covering all audits, together with the scope of each Audit, and shall submit such an Audit Schedule to TfL for Assurance prior to the Planned Operational Commencement Date.		

Z.4.3.11		Mandatory
The Service Provider shall submit to TfL for Approval, the proposed security audits to be carried out and, when Approved, carry out such security audits in accordance with Schedule 14: Security.		

Z.4.3.12		Mandatory
The Service Provider shall carry out a privacy audit on all of the Service System(s) in accordance with BS10012, and guidance from the Information Commissioner's Office - ICO Guide to Data Protection Audits.		

Z.4.3.13		Mandatory

The Service Provider shall share the results of any privacy and/or security audit carried out with TfL.

Z.4.3.14		Mandatory
The Service Provider shall implement the recommendations from any audits within the timescales agreed with TfL.		

4.4 Digital Certificates

Z.4.4.1		Mandatory
The Service Provider shall provide Certification Authority services in respect of all Service Elements, including issuing, verifying and revoking Digital Certificates.		

Z.4.4.2		Mandatory
In its role as the Certification Authority for the Service Systems, on request from TfL the Service Provider shall issue Digital Certificates for the Service System(s) to TfL and Third Parties.		

4.5 Security

Z.4.5.1		Mandatory
The Service Provider shall construct the Service System(s) such that unexpected and erroneous Data inputs do not in any way expose the Service System(s) source code, and memory content to the User.		

Z.4.5.2		Mandatory
The Service Provider shall ensure that all Bespoke Software releases are in accordance with Schedule 14: Security		

Z.4.5.3		Mandatory
The Service Provider shall ensure that scanning of all new software releases is performed by an independent security auditor prior to implementation.		

Z.4.5.4		Mandatory
The Service Provider shall ensure that all network connections within the Service System, including those for staff access, are provided on a secure network used solely for the purposes of performing the Services under this Agreement.		

Z.4.5.5		Mandatory
The Service Provide shall ensure that the network used in the performance of the Services under this Agreement is not directly connected with the Service Provider's own in house network.		

Z.4.5.6		Mandatory
The Service Provider shall ensure that only the Service Provider's Service System authorised administrators have the capability to define User roles and to assign Users to those roles.		

Z.4.5.7		Mandatory
The Service Provider shall conduct Ready for Service Testing (in accordance with Schedule 4: Testing Regime) at TfL's request after a Security Audit, Release, or a Change has been implemented.		

Z.4.5.8		Mandatory
The Service Provider shall ensure that the Service System(s) have the functionality to prevent cross-site scripting attacks.		

4.6 Security incident and event management solution

Z.4.6.1		Mandatory
The Service Provider shall implement an appropriately certified software tool for Security Incident and Event Management and shall submit the details of the tool to TfL for Assurance before the Operational Commencement Date and, when Assured, shall implement and operate such tool.		

Z.4.6.1b		Mandatory
The Service Provider shall develop processes and procedures for Security Incident and Event Management and shall submit such processes and procedures to TfL for Assurance in accordance with this Statement of Requirements and the Schedule 2: Statement of Requirements (MIS) before the Operational Commencement Date and, when Assured, implement and comply with such processes and procedures.		

Z.4.6.1c		Mandatory
The Service Provider shall upon request supply TfL with the relevant logs in a human readable format to investigate any potential Security Incident or event.		

Z.4.6.2		Mandatory
The Service Provider shall develop and comply with a Security Incident and Event Management ("SIEM") solution and shall submit such a solution to TfL for Assurance, prior to the Operational Commencement Date of the Service System(s) and maintain the SIEM throughout the duration of the contract.		

Z.4.6.3		Mandatory
The SIEM solution shall aggregate data from the Service System(s) sources, including without limitation: • Network;		

- firewalls;
- servers;
- databases; and
- applications.

Z.4.6.4		Mandatory
The Service Provider shall ensure that the SIEM solution identifies common data attributes and links events together into meaningful bundles such that correlation techniques may be applied to integrate the different sources and interpret the data into security event information.		

Z.4.6.5		Mandatory
The Service Provider shall ensure that the SIEM solution automatically analyses correlated events and sends alerts to the Service Provider's Security Manager and/or relevant personnel immediately.		

Z.4.6.6		Mandatory
The Service Provider shall ensure that the SIEM solution analyses and represents event data in informational chart format to assist pattern identification and to highlight any activities that do not conform to a standard pattern.		

Z.4.6.7		Mandatory
The Service Provider shall ensure that the SIEM solution automatically gathers information about Compliance Data and generates reports suitable for security, governance and auditing processes.		

Z.4.6.8		Mandatory

The Service Provider shall ensure that the SIEM solution stores historical Data long-term to facilitate correlation of Data over time and to provide the retention necessary to satisfy compliance requirements in accordance with Appendix 11: Data Retention.

Z.4.6.9		Mandatory
The Service Provider shall transfer all aggregated and historical SIEM Data to a secure location.		

Z.4.6.10		Mandatory
The Service Provider shall develop and comply with a format for delivery of all aggregated and historical SIEM Data and shall submit such a format to TfL for Assurance.		

Z.4.6.11		Mandatory
The Service provider shall ensure that all aggregated and historical SIEM Data is secured with ‘read only’ access.		

Z.4.6.12		Mandatory
The Service Provider shall develop and comply with a method by which aggregated and historical SIEM Data is to be secured in a ‘read only’ format and shall submit such a method to TfL for Assurance.		

Z.4.6.13		Mandatory
The Service Provider shall ensure that the SIEM solution mitigates the effect of any potential and actual breach of security.		

Z.4.6.14		Mandatory
The Service Provider shall ensure that no User assigned to a SIEM role is concurrently assigned to a systems administration role. For the avoidance of doubt the systems administration role includes but is not limited to: • Data base administration (DBA);		

- User account maintenance;
- Maintenance of system files such as system logs, backup files and various data extracts provided to TfL;
- Network maintenance including any security and communications software; and
- Hardware maintenance.

5. TESTING

This section covers those requirements relating to Testing including Test Process and Test Environments and should be read in conjunction with Schedule 4: Testing Regime and Schedule 3: Milestones and Deliverables.

5.1 General

Z.5.1.1		Mandatory
The Service Provider shall carry out Testing in accordance with Schedule 4: Testing Regime.		

6. SERVICE MANAGEMENT

This section covers the areas of Service Management for the purposes of provisioning and managing the Service System(s).

6.1 General

Z.6.1.1		Mandatory
The Service Provider shall implement methods, processes, procedures and tools for Service Management on the Operational Commencement Date of the Agreement. Such methods, processes, procedures and tools shall be submitted to TfL for Assurance prior to being implemented.		

Z.6.1.2		Mandatory
The Service Provider shall develop and comply with processes, procedures and tools used to perform Service Management and shall submit such processes and procedures to TfL for Assurance by the Milestone Date for Milestone [•] (Ready to Commence Service Proving Date).		

Z.6.1.3		Mandatory
The Service Provider shall develop and comply with a process to automatically register and update each Change, Incident, Problem, and Service Request in TfL's Service Desk and shall submit such a process to TfL for Assurance.		

6.2 Capacity Planning

Z.6.2.1		Mandatory
The Service Provider shall design the Service System(s), and all constituent parts of it, to be capable of being scaled smoothly from the initial deployment, which supports only the defined Services in this Agreement, to support Services with up to two (2) times the current steady state operational volumes as set out in Appendix 03 :Volumetrics (Business		

Operations), without Changes to the overall Service System(s) design or the design of any constituent parts of the Service System(s) (Hardware, Firmware or Software) except for increasing the Capacity of the Hardware and Software configuration.

Z.6.2.2		Mandatory
The Service Provider shall build and implement the Service System(s) to be scalable, configurable to one and a half (1.5) times the initial volumetric requirements outlined in Appendix 03: Volumetrics and without the need to Change any Hardware.		

Z.6.2.3		Mandatory
The Service Provider shall ensure that there is available Capacity to meet the Service Levels as specified in Schedule 5 : Service Level Agreement for the Service System(s).		

Z.6.2.4		Mandatory
The Service Provider shall provide the Capacity Plan(s) to TfL for Assurance prior to the implementation of the Service System(s).		

Z.6.2.5		Mandatory
The Service Provider shall update the Capacity Plan(s) to reflect the Service System(s) performance in relation to projected volumes as specified in Appendix 03: Volumetrics		

Z.6.2.6		Mandatory
The Service Provider shall review and maintain the Capacity Plan(s) at intervals of not more than six (6) months, in the event of a Change Control Request and at the request of TfL, to reflect Service System(s) performance in relation to volume, technical and operational changes and future volume projections in accordance with Clause 17.		

Z.6.2.7		Mandatory

The Service Provider shall at its cost provide a Change Control Request in accordance with Schedule 9: Change Control Request Procedure for any increases in Capacity where the Service Provider predicts Capacity to be insufficient to meet demand.

Z.6.2.8		Mandatory
The Service Provider shall track and report actual consumption against projections from prior Capacity Plans at intervals to be agreed with TfL.		

6.3 Configuration Management

Z.6.3.1		Mandatory
The Service Provider shall maintain all components of the Service System(s) under Configuration Management in accordance with Good Industry Practice.		

Z.6.3.2		Mandatory
The Service Provider shall develop and comply with a Configuration Management Solution that manages relationships between Configuration Items and shall submit such a solution to TfL for Assurance.		

Z.6.3.3		Mandatory
The Service Provider shall ensure that the Configuration Management Solution prevents Configuration Item records from being updated without the appropriate change approvals and procedures being followed.		

Z.6.3.4		Mandatory
The Service Provider shall ensure that the Configuration Management Solution displays the current status of Configuration Items.		

Z.6.3.5		Mandatory

The Service Provider shall ensure that the Configuration Management Solution verifies that correct and authorised versions of Configuration Items exist.

Z.6.3.6		Mandatory
The Service Provider shall ensure that the Configuration Management Solution identifies and logs Configuration Items that are affected when related Configuration Items are the subject of: • an Incident; • a Defect; and • Change.		

Z.6.3.7		Mandatory
The Service Provider shall ensure that the Configuration Management Solution updates the version number of a Configuration Item if any amendments are made to the Configuration Item with the previous version number.		

Z.6.3.8		Mandatory
The Service Provider shall ensure that the Configuration Management Solution retains historic details in accordance with Appendix 11: Data Retention of all Configuration Items including, but not limited to: • installation date of the Configuration Item • records of changes to the Configuration Item; and • locations of the Configuration Item.		

Z.6.3.9		Mandatory
The Service Provider shall ensure that the Configuration Management Solution supports the management and use of baseline versions that can be used for reverting to a previous complete and known to be a working version.		

Z.6.3.10		Mandatory
The Service Provider shall ensure that the Configuration Management Solution generates reports on the inventory of Configuration Items.		

Z.6.3.11		Mandatory
The Service Provider shall be able to produce reports upon request from TfL from any of the data fields that are held within the Configuration Management Solution.		

Z.6.3.12		Mandatory
The Service Provider shall ensure that the Configuration Management Solution validates user input to ensure that all fields flagged as mandatory have been completed. The list of mandatory fields shall be configurable.		

6.4 Change Process

Z.6.4.1		Mandatory
The Service Provider shall manage the Change Process in accordance with Schedule 9: Change Control Procedure.		

6.5 Incident Management

Z.6.5.1		Mandatory
The Service Provider shall manage the Incident Management Process in accordance with Clause 12.		

Z.6.5.2		Mandatory
The Service Provider shall ensure that TfL is able to call and log Incidents with the Service System(s) twenty four (24) hours a day, seven (7) days a week, three hundred and sixty five (365) days a year.		

Z.6.5.3		Mandatory
The Service Provider shall raise a Severity 1 Incident when the reconciliation of Data fails, until the underlying root-cause is determined and a lower Severity Level is agreed with TfL.		

Z.6.5.4		Mandatory
The Service Provider shall raise a Severity 1 Incident when any payment channel fails, until the underlying root-cause is determined and a lower Severity Level is agreed with TfL.		

Z.6.5.5		Mandatory
The Service Provider shall raise a Severity 1 Incident when server loads significantly impede the performance of the Service Systems, until the underlying root-cause is determined and a lower Severity Level is agreed with TfL.		

Z.6.5.6		Mandatory
The Service Provider shall raise a Severity 1 Incident when Interfaces fail, until the underlying root-cause is determined and a lower Severity Level is agreed with TfL.		

Z.6.5.7		Mandatory
The Service Provider shall raise a Severity 1 Incident when any network connectivity fails, until the underlying root-cause is determined and a lower Severity Level is agreed with TfL.		

Z.6.5.8		Mandatory
The Service Provider shall be responsible for the resolution of all Incidents in accordance with Clause 12.		

Z.6.5.9		Mandatory
The Service Provider shall be responsible for working with Other Service Providers, in accordance with Clause 15: Co-operation with TfL and Others, to resolve Incidents where the failure may lie outside the scope of the Services or where a failure may impact Other Service Provider's operations.		

Z.6.5.10		Mandatory
The Service Provider shall develop and comply with escalation procedures for resolution of Incidents and shall submit such procedures to TfL for Assurance where these are, or are suspected to be, related to: • the Service System(s); • Third Parties' Systems; and • the Interfaces.		

Z.6.5.11		Mandatory
Where an Incident is considered by the Service Provider to result from an act or omission of a Sub-Contractor or an Other Service Provider, the Service Provider shall manage such Incident in accordance with Clauses 12 and 15.		

Z.6.5.12		Mandatory
The Service Provider shall bear the cost of any work undertaken by a Third Party in order to resolve an Incident within the scope of the Services, where the Service Provider has failed to perform this work itself or has attempted to perform this work and been unsuccessful.		

Z.6.5.13		Mandatory
The Service Provider shall provide TfL with direct read-only access to the electronic Incident Log on request.		

Z.6.5.14		Mandatory
The Service Provider shall provide TfL with reports, in electronic format when requested by TfL, from the Incident Log including full details of: • Incidents; • Security Incidents;		

• Changes; and • Any other incidents.

Z.6.5.15		Mandatory
The Service Provider shall nominate an Incident resolution and/or problem manager for each Incident.		

Z.6.5.16		Mandatory
The Service Provider shall log the corrective actions taken to resolve Incidents in the Incident Log.		

Z.6.5.17		Mandatory
The Service Provider shall distinguish between: • Incidents; • Defects; • Changes; • Security Incidents; • Performance Indicator Incidents and; • Closed, where the Incident is deemed to be in none of these classifications.		

Z.6.5.18		Mandatory
The Service Provider shall classify Incidents, Defects, Changes, Security Incident and Performance Indicator Incidents by Severity Level Incidents, in accordance with the Severity Levels set out in Schedule 1: Definitions.		

Z.6.5.19		Mandatory
The Service Provider shall respond to Incidents within the following timescales according to their Severity Level:		

- Severity 1 – fifteen (15) minutes;
- Severity 2 – one (1) hour;
- Severity 3 – three (3) hours;
- Severity 4 – eight (8) hours; and
- Severity 5 – ten (10) hours.

Z.6.5.20		Mandatory
The Service Provider shall resolve Severity 1, Severity 2, and Severity 3 Incidents in accordance with the timescales set out in Schedule 5: Service Level Agreement.		

Z.6.5.21		Mandatory
The Service Provider shall report progress on any Severity 1 or Severity 2 Incidents to TfL every thirty (30) minutes until the Incident is resolved.		

Z.6.5.22		Mandatory
The Service Provider shall report progress on any Severity 3 Incident each Working Day until the Incident is resolved.		

Z.6.5.23		Mandatory
The Service Provider shall report progress on any Severity 4 and Severity 5 Incident at an interval to be agreed with TfL.		

Z.6.5.24		Mandatory
The Service Provider shall resolve any Severity 4 and Severity 5 Incident in the timeframe Agreed with TfL		

Z.6.5.25		Mandatory

The Service Provider shall analyse the Incident Log to identify common recurring Incidents, Defects, Security Incidents and Performance Indicator Incidents and take such action as has been agreed with TfL to prevent their re-occurrence.

Z.6.5.26		Mandatory
The Service Provider shall identify Incident(s) that require a Change and create a Change Request(s) in accordance with Schedule 9: Change Control Request Procedure, and shall close these Incidents in the Incident Log.		

Z.6.5.27		Mandatory
The Service Provider shall at TfL's request re-evaluate any Incident. In the event of a disagreement between TfL and the Service Provider over the classification of an Incident or the assignment of a Severity Level, it shall be referred to the next Commercial Meeting. If an agreement cannot be reached at the Commercial Meeting then the Service Provider shall follow TfL's instructions on the classification of the Incident and assignment of a Severity Level.		

Z.6.5.28		Mandatory
If an Incident cannot be resolved within the resolution time periods as specified for its Severity Level as detailed in Schedule 5: Service Level Agreement the Service Provider shall deliver to TfL for Approval a Remedy Plan in accordance with Clause 58.		

Z.6.5.29		Mandatory
The Service Provider shall provide a weekly Incident report to TfL prior to the Commercial Meeting. This shall include: • a description of all Incidents arising in the previous week, together with their classification and their Severity Level in the case of Incidents, Defects, Security Incidents and Performance Indicator Incidents; • a status report on all open Incidents Defects, Security Incidents and Performance Indicator Incidents; and		

- a description of the resolution of all Incidents, Defects, Security Incidents and Performance Indicator Incidents closed during the previous week.

Z.6.5.30		Mandatory
The Service Provider shall link similar Incidents, Defects, Security Incidents and Performance Indicator Incidents to Problems.		

Z.6.5.31		Mandatory
The Service Provider shall track and keep a record of the total amount of time spent resolving each Incident, Defects, Security Incidents and Performance Indicator Incidents and how long it was open.		

Z.6.5.32		Mandatory
The Service Provider shall be able to report on Incidents linked to Problems.		

Z.6.5.33		Mandatory
The Service Provider shall analyse and report on trends of Incidents.		

Z.6.5.34		Mandatory
The Service Provider shall ensure the time to resolve an Incident is the time from any person raising the Incident to the time the Incident is resolved and closed. An Incident is considered to be resolved and closed when corrective action has been completed, Tested and the Incident properly recorded as closed in the Issue Management Log by the Service Provider with the express written agreement of TfL, which agreement may be given retrospectively.		

Z.6.5.35		Mandatory
The Service Provider shall ensure that the time at which an Incident is logged in the Incident Log is the earliest of: (i) an alarm being generated by any element of the Service System(s); (ii) notification of an Incident being provided to the Service Provider;		

(iii) any of the applications or Services becoming unavailable; or

(iv) where an Incident is raised by Service Provider Personnel.

Z.6.5.36		Mandatory

The Service Provider shall ensure that the Performance Indicator shall be measured for each Incident arising, regardless of Severity. The required fix time for each Severity is set out in this Statement of Requirements in the table below:

Performance Indicator title	**Start Point**	**End Point**	**Acceptable Service Level**	**Band 1**	**Band 2**	**Band 3**
Adherence to Fix Times	The time at which the incident is logged	The time at which the Severity 1 incident is resolved and closed	Severity 1 < 4 hours	1,500 per incident	3,000 per incident	50,000 points (fixed)
				24-48 hours	>48-72 hours	>72 hours
Adherence to Fix Times	The time at which the incident is logged	The time at which the Severity 2 incident is resolved and closed	Severity 2 < 24 hours	1,500 per incident	3,000 per incident	50,000 points (fixed)
				3-4 months	>4-6 months	>6 months
Adherence to Fix Times	The time at which the	The time at which the	Severity 3 < 3 calendar	1,500 per incident	3,000 per incident	6,000 per incident

		incident is logged	Severity 3 incident is resolved and closed	months or next closest maintenance release date				

6.6 Release Management

Z.6.6.1		Mandatory
The Service Provider shall develop and comply with a Release Management process and shall submit such a process to TfL for Assurance.		

Z.6.6.2		Mandatory
The Service Provider shall ensure that the Release Management process includes but is not limited to: • Hardware; • Software; • License renewals; • Configuration Items; and • all changes to Parameters and processes.		

Z.6.6.3		Mandatory
The Service Provider shall produce Release Notes to be provided to TfL before a Release is deployed to an Environment.		

Z.6.6.4		Mandatory
The Service Provider shall ensure that the Release Notes include but are not limited to: • A description of any new or amended functionality; • Any known errors and Defects remaining in the release; and • Any operational workarounds required due to those errors and Defects.		

Z.6.6.5		Mandatory
The Service Provider shall ensure that all Hardware, Software, Licence renewals, Configuration Items and changes to Parameter and processes involved in the delivery of the Services are under the control of the Release Management process, and these shall only be updated through formal Release.		

Z.6.6.6		Mandatory
The Service Provider shall document the contents of a Release before it is deployed to an Environment.		

Z.6.6.7		Mandatory
The Service Provider shall ensure that the Release Management process tracks, for each Release, at least the following items: • a unique identifier; • the identity of any individual involved in the Workflow surrounding a deployment, including requesting, approving or executing it; and • the dates on which the Release was deployed into the Service System(s).		

Z.6.6.8		Mandatory
The Service Provider's shall ensure that the Release Management process distinguishes between the following types of Releases: • major; • minor; and • emergency.		

Z.6.6.9		Mandatory
The Service Provider shall ensure that the Release Management process supports control mechanisms for building different types of Releases. This shall include visibility of the stages		

of the Software build and evidence that all relevant policies, regulations and standards have been followed.

Z.6.6.10		Mandatory
The Service Provider shall ensure that the Release Management process assesses the risks associated with each Release, including without limitation: • impact; • probability of occurrence; • proposed mitigations; and • contingencies.		

Z.6.6.11		Mandatory
The Service Provider shall ensure that the Release Management process tracks and records the Release lifecycle stage including, without limitation: • build; • test; • deployment; and • close.		

Z.6.6.12		Mandatory
The Service Provider shall prevent further progression of the Release in the event that the Release or any part of the Release fails at any stage in the Release process and immediately informs TfL of such failure.		

Z.6.6.13		Mandatory
The Service Provider shall ensure that the Release Management process supports the planning of Release activities including but not limited to training, deliveries, transition environments, and staffing.		

Z.6.6.14		Mandatory
The Service Provider shall report on the number of Releases: • over any given period requested by TfL; • that are active and planned; • that are closed; and • by category.		

Z.6.6.15		Mandatory
The Service Provider shall keep a secure audit log of all Release updates and closure dates and times.		

6.7 Performance

Z.6.7.1		Mandatory
The Service Provider shall provide and maintain all Service System(s) to ensure that the Service Levels can be achieved at all times in accordance with Schedule 5: Service Level Agreement.		

6.8 Maintenance Support

Z.6.8.1		Mandatory
The Service Provider shall ensure that no Service System(s) downtime occurs when System maintenance is undertaken, unless previously agreed and Scheduled with TfL		

Z.6.8.2		Mandatory
The Service Provider shall ensure that regular preventative maintenance is carried out across all Service System(s).		

Z.6.8.3		Mandatory

The Service Provider shall maintain a plan of regular preventative maintenance activities for at least a six (6) month future period in accordance with Clause 19: Systems, Support and Maintenance

Z.6.8.4		Mandatory
The Service Provider shall provide its proposed plan for regular preventative maintenance activities to TfL for Assurance in accordance with Clause 19: Systems, Support and Maintenance		

Z.6.8.5		Mandatory
The Service Provider shall agree any extraordinary maintenance activities that are additional to the Assured plan of regular preventative maintenance with TfL at least two (2) days prior to carrying out the maintenance activities in accordance with Clause 19		

Z.6.8.6		Mandatory
The Service Provider shall ensure that all Hardware, Software and Equipment used as part of the Service System(s) is maintained at a supported production release at no cost to TfL.		

Z.6.8.7		Mandatory
The Service Provider shall Schedule preventative maintenance to address Incidents, Defects, Problems, Security Incidents and Performance Indicator Incidents as part of the regular maintenance plan, where appropriate.		

Z.6.8.8		Mandatory
The Service Provider shall ensure that all upgrades to COTS Products are agreed with TfL (prior to being implemented in the Service System(s)) in accordance with Schedule 9: Change Control Request Procedure.		

6.9 Quality Assurance

Z.6.9.1		Mandatory
The Service Provider shall develop and comply with a Quality Assurance process and shall submit such a process to TfL for Assurance		

Z.6.9.2		Mandatory
The Service Provider shall develop a Quality Plan, that: • ensures that all aspects of the Services are the subject of quality management systems; and • is consistent with ISO 9001:2005 or any standard which is generally recognised as being equivalent to it.		

Z.6.9.3		Mandatory
The Service Provider shall submit to TfL for Approval the date by which it can deliver the Quality Plan, prior to the Operational Commencement Date and, once Approved, shall deliver the Quality Plan on or before such Approved date.		

Z.6.9.3b		Mandatory
The Service Provider shall submit the Quality Plan to TfL for Assurance within the Approved timescale, and once Assured, comply with the Quality Plan.		

Z.6.9.4		Mandatory
The Service Provider shall provide the Services in accordance with the Quality Plan		

Z.6.9.5		Mandatory
The Service Provider shall develop and comply with a Quality Plan and shall submit such a Quality Plan together with any proposed changes to TfL for Assurance		

Z.6.9.6		Mandatory
The Service Provider shall ensure continuity in the management of quality assurance		

during the term of the Agreement

6.10 Systems Monitoring

Z.6.10.1		Mandatory
The Service Provider shall monitor and operate in accordance with Schedule 5: Service Level Agreement, Schedule 10: Contract Management and Reporting, Schedule 14: Security and Schedule 34: TfL Policies and all other terms of this Agreement the following: • Service System(s) and their resources; • Service System performance; • Interfaces and their resources; • Interface performance; • Networks and their resources; • Network performance; • device utilisation; • Incident, Problem and Defect rates; and • System logs.		

Z.6.10.2		Mandatory
The Service Provider shall use appropriate tools to monitor and manage the Service System(s) performance, including, but not limited to: • System availability; • Interface performance; • server load; and • network load.		

Z.6.10.3		Mandatory

The Service Provider shall provide a comprehensive Service Monitoring System with the capability to monitor the status of all components of the Service System(s) and Infrastructure and to raise alarms in the event of component failure, Service System(s) performance degradation and any other potential issues that affect the operation and performance of the Services.

Z.6.10.4		Mandatory
The Service Provider shall ensure that the Service Monitoring System runs continuously twenty four (24) hours a day, seven (7) days a week, 365 days a year and any alarms are immediately raised on the Service Monitoring System.		

Z.6.10.5		Mandatory
The Service Provider shall ensure that its support personnel are notified of alarms raised on the Service Monitoring System. This shall include the provision of notifications by SMS and email.		

Z.6.10.6		Mandatory
The Service Provider shall provide mechanisms to ensure that alarms from the Service Monitoring System are received by the Service Provider’s nominated Personnel at any Premises and at any time.		

Z.6.10.7		Mandatory
The Service Provider shall continuously and automatically monitor all Interfaces for the following including, but not limited to: • availability; • throughput; • performance; • buffer usage;		

- queue lengths;
- Hardware status;
- System alarms and warnings; and
- any other diagnostic Data provided by the Service Provider's implementation of the Interfaces.

Z.6.10.8		Mandatory
The Service Provider shall categorise System Events into the following categories (but not limited to): • required for information; • a warning; • a failure; and • an exception.		

Z.6.10.9		Mandatory
The Service Provider shall ensure that the Service Monitoring System has the capability to prioritise System Events		

6.11 Reporting

Z.6.11.1		Mandatory
The Service Provider shall provide reporting facilities and reports which permit TfL to monitor the performance of the Service System(s) in accordance with Schedule 10: Contract Management and Reporting, and Schedule 2: Statement of Requirements (MIS).The Service Provider shall provide User guides and describe the underlying data so performance queries and reports can be constructed by TfL staff.		

Z.6.11.2		Mandatory
The Service Provider shall provide Asset management reports in accordance with		

Schedule 10: Contract Management and Reporting and Schedule 12: Asset Management.

Z.6.11.3		Mandatory
The Service Provider shall provide TfL with monthly reports on all maintenance activities undertaken in the previous month.		

Applicable from the ULEX Operational Commencement Date		
Z.6.11.4		Mandatory
The Service Provider shall make available to TfL on request such standard reports as are available and utilised by the Services Provider (whether developed by the Service Provider or available as standard from the Cloud Service Provider) provided the (a) relate specifically to the Service Provided under this Agreement; and (b) would not cause the Service Provider to breach its confidentiality obligations as detailed in Clause 37.6.		

6.12 Incident Management

Z.6.12.1		Mandatory
The Service Provider shall minimise the number of Incident Logs for the Service System(s) in order to facilitate visibility and management of the Incidents		

6.13 Problem Management

Z.6.13.1		Mandatory
The Service Provider shall develop and comply with a Problem Management Solution, in accordance with the Service Management framework, and shall submit such solution to TfL for Assurance.		

Z.6.13.2		Mandatory
The Service Provider shall not close a Problem until all related Incidents have been resolved in accordance with this Agreement.		

Z.6.13.3		Mandatory
The Service Provider shall track the total amount of time the Problem was worked on and how long it was open.		

Z.6.13.4		Mandatory
The Service Provider shall assign Severity Levels, impact, and priorities to Problems.		

Z.6.13.5		Mandatory
The Service Provider shall report on the number of Problems by Severity Level, impact, and priority.		

Z.6.13.6		Mandatory
The Service Provider shall report on the number of Problems per month that are: • Closed; • Open; and • in progress.		

Z.6.13.7		Mandatory
The Service Provider shall report on a monthly basis on the number of Problems reopened.		

Z.6.13.8		Mandatory
The Service Provider shall report on a monthly basis on the number of related Incidents occurring before a Problem is closed.		

6.14 Logging

Z.6.14.1		Mandatory
The Service Provider shall log all Service System(s) failures, errors and execution of		

scheduled processes immediately.

Z.6.14.2		Mandatory
The Service Provider shall not carry out any Service System(s) Monitoring actions without a documented procedure. Where a required action is not documented in a procedure, the Service Provider shall log the action before action is allowed to be taken, and update the Service Systems(s) processes and procedures to reflect the action taken.		

Z.6.14.3		Mandatory
The Service Provider shall ensure that all Service System(s) diagnostic messages and alarms provide at least the following information: • date and time; • name or ID of the affected component; and • status message.		

Z.6.14.4		Mandatory
The Service Provider shall record status information received from the Service System(s) in a System log. Certain Service System(s) may be excluded from this requirement with TfL's prior written consent.		

Z.6.14.5		Mandatory
The Service Provider shall retain all Service System(s) Logs in accordance with the Agreement or as agreed with TfL from time to time.		

Z.6.14.6		Mandatory
During the Operational Phase, the Service Provider shall ensure that the Service System(s) Log is signed daily by the Service Provider's Personnel responsible for managing the provision of the Services on that day.		

6.15 Service Level Management

Z.6.15.1		Mandatory
The Service Provider shall manage the Service System(s) and Service to meet the Service Levels as stated in Schedule 5: Service Level Agreement.		

6.16 Network and Service System(s) Resilience

Z.6.16.1		Mandatory
The Service Provider shall ensure that it provides Network and Service System(s) resilience which prevents failures across all Service System Elements such as Networks, routers, switches, firewalls, transmission interconnections for both local area and wide area networks, servers and disks.		

Z.6.16.2		Mandatory
The Service Provider shall ensure that the Service System(s) has the functionality to switch to an alternative power supply so that no degradation of Service occurs.		

Z.6.16.3		Mandatory
The Service Provider shall ensure that the Service System(s) has the functionality to switch to a standby working Service System Element or load sharing, so that the failure of a single Service System Element within a group of similar Service System Elements does not cause degradation of Service.		

Z.6.16.4		Mandatory
The Service Provider shall ensure that the Network and the Service System(s) has the functionality to automatically switch to standby ancillary network working Service System Elements or load sharing, such that the failure of a single ancillary network Service System Element within a group does not cause degradation of Service.		

Z.6.16.5		Mandatory
The Service Provider shall ensure that Network elements and transmission interconnections allow for one hundred and fifty per cent (150%) above the volumes set out in Appendix 03: Volumetrics		

7. SERVICE SYSTEM(S)
This section sets out certain requirements relating to Service System(s).
7.1 Operational Processes and Procedures

Z.7.1.1		Mandatory
The Service Provider shall build the Service System(s) in accordance with Schedule 3: Milestones and Deliverables, Schedule 28: Service Provider's Solution.		

Z.7.1.2		Mandatory
The Service Provider shall implement a MIS solution in accordance with Schedule 2: Statement of Requirements (MIS).		

Z.7.1.3		Mandatory
The Service Provider shall not customise any COTS products which may render the product unsupportable under the vendor's standard support package		

Z.7.1.4		Mandatory
The Service Provider shall provide and maintain a common standard build for all workstations used in the provision of the Service System(s).		

Z.7.1.5		Mandatory
The Service Provider shall ensure that all Software, Hardware, and Information installed on workstations and servers used in the provision of the Service System(s) are for business purposes only		

Z.7.1.6		Mandatory
The Service Provider shall ensure that the hosted elements of the Service Systems are segregated from the Service Provider's other customer hosted services, are secure and		

can only be accessed or viewed by Operational Users in accordance with this Agreement.

Z.7.1.7		Mandatory
The Service Provider shall procure all Hardware to be used within the Service System(s) from a reputable manufacturer offering a support capability		

Z.7.1.8		Mandatory
The Service Provider shall design the Service System(s) to prevent Users from violating Privacy Legislation		

Z.7.1.9		Mandatory
The Service Provider shall store used digital media for a minimum of six (6) months before destruction in accordance with Schedule 14: Security and Appendix 11: Data Retention		

Z.7.1.10		Mandatory
The Service Provider shall ensure that all digital media is labelled clearly by the date and times of recording.		

Z.7.1.11		Mandatory
The Service Provider shall ensure that all digital media is stored in chronological order by recording date and time.		

Z.7.1.12		Mandatory
The Service Provider shall ensure that all digital media is available for viewing at any time on demand by TfL.		

Z.7.1.13		Mandatory
The Service Provider shall ensure that all digital media is made available for full audits of access requests and use.		

7.2 Service System Functions

Z.7.2.1		Mandatory
The Service Provider shall develop and comply with a mechanism containing the features and functionality of a mechanism to allow wildcard searches on search fields and shall submit such mechanism to TfL for Assurance		

Z.7.2.2		Mandatory
The Service Provider shall make use of a Parameterised Change Element, to facilitate the maintenance of the Service System(s) and future Changes to the Services and Service System(s).		

Z.7.2.3		Mandatory
The Service Provider shall ensure that the following Parameterised Change Elements are not hard coded within the Service System(s). These values include, without limitation: • codes; • statuses; • dates; • times; • percentages; • monetary values; • operational hours and days; • reference Data; and • other parameters. In the event that solution components do not meet this requirement, the Service Provider shall not be afforded any performance or financial relief under the Schedule 9: Change Control Request Procedure		

Z.7.2.4		Mandatory
The Service Provider shall develop and comply with a proposed list of Parameterised Change Elements and shall submit such a list to TfL for Assurance.		

Z.7.2.5		Mandatory
The Service Provider shall allow each Parameterised Change Element to be varied by value and variety using a Parameter Driven configuration approach.		

Z.7.2.6		Mandatory
The Service Provider shall store each Parameterised Change Element centrally, for example in parameter tables.		

Z.7.2.7		Mandatory
The Service Provider shall ensure that each Parameterised Change Element can be configured by all Service Provider Personnel and at no cost to TfL.		

Z.7.2.8		Mandatory
The Service Provider shall ensure that any Change to a Parameterised Change Element is in accordance with Schedule 9: Change Control Request Procedure.		

7.3 Backup

Z.7.3.1		Mandatory
The Service Provider shall ensure that the Service System(s) Data can be recovered from loss and corruption back to any point in time.		

Z.7.3.2		Mandatory
The Service Provider shall provide a data archiving function. This function will also be used to ensure that data is available and recoverable in accordance with Appendix 11: Data Retention		

7.4 Shutdown/Start-up Processes

Z.7.4.1		Mandatory
The Service Provider shall ensure that Planned Downtime takes place in accordance with Schedule 5: Service Level Agreement, and Clause 46.3 unless otherwise Approved by TfL and implemented within the timescales stipulated by TfL.		

Z.7.4.2		Mandatory
The Service Provider shall develop, maintain and follow a documented procedure for Service Systems start-up and shut-down. If it becomes necessary to deviate from the procedure, the Service Provider shall raise this as an Incident.		

Z.7.4.3		Mandatory
The Service Provider shall ensure a number of Personnel are trained in following the Service System(s) shut down and start up procedures and tools and that the Personnel are readily available to enable execution at any time.		

Z.7.4.4		Mandatory
The Service Provider shall raise all unscheduled shut down or loss of any Service System(s), for any reason, as a Severity 1 Incident.		

Z.7.4.5		Mandatory
The Service Provider shall perform Tests annually to ensure Service System(s) shut down and start up procedures operates correctly.		

7.5 Time

Z.7.5.1		Mandatory
The Service Provider shall ensure all system clocks are consistent with Co-ordinated		

Universal Time (UTC) and are adjusted to conform to Daylight Savings Time (DST) when in effect.

Z.7.5.2		Mandatory
In the event that the NTP Time Server is unavailable the Service Provider shall provide a standby GPS receiver to synchronise Co-ordinated Universal Time (UTC).		

Z.7.5.3		Mandatory
The Service Provider shall ensure that the Service System(s) provide the appropriate sequencing and timestamps to the TfL Website for each transaction.		

8. BUSINESS CONTINUITY

This section covers those requirements which shall apply to ensure continuity of business operations in the event of a 'disaster' which prevents service operations at the normal operational sites.

8.1 Business Continuity

Z.8.1.1		Mandatory
The Service Provider shall prepare, implement and maintain a Business Continuity Plan and provide Business Continuity Infrastructure in accordance with Schedule 25: Business Continuity.		

8.2 Asset Management

Z.8.2.1		Mandatory
The Service Provider shall produce and maintain an Asset Management System with appropriate details in accordance with Schedule 12: Asset Management.		

Z.8.2.2		Mandatory
The Service Provider shall ensure that the Asset Management System provides a range of reporting in accordance with Schedule 12: Asset Management.		

Z.8.2.3		Mandatory
The Service Provider shall ensure that the Asset Management System provides flat file output to allow Data to be exported to a future Asset Management system.		

Z.8.2.4		Mandatory

The Service Provider shall ensure that the Asset Management System triggers alerts when renewals are due for software license agreements. The frequency, format, and method of alerting shall be configurable.

Z.8.2.5		Mandatory
The Service Provider shall ensure that the Asset Management System has the capability to take asset lifecycle information feeds from different sources to trigger events such as end of life dates for hardware and software.		

Z.8.2.6		Mandatory
The Service Provider shall develop and comply with an Asset Management System to monitor usage patterns of software to support the re-deployment of software licences and to identify potentially redundant licences including the provision of a monthly report and shall submit such a system including the format of the monthly report to TfL for Assurance.		

Z.8.2.7		Mandatory
The Service Provider shall ensure that the Asset Management System supports both automated and manual updates of asset information.		

Z.8.2.8		Mandatory
The Service Provider shall ensure that the Asset Management System has the capability to alert groups by email.		

9. DATA

This section covers those requirements which apply to the service data and cover general data aspects, data migration and data migration and reference data.

9.1 Data Migration Planning

Z.9.1.1		Mandatory
The Service Provider shall provide the proposed Data Migration Strategy to TfL to be Approved in accordance with Schedule 3: Milestones and Deliverables.		

Z.9.1.2		Mandatory
The Service Provider shall submit to TfL for Approval a date by which it shall provide the Level 1 Data Migration Plan to TfL prior to the Milestone Date for Milestone [•] (Mobilisation Complete Date) and, once Approved, deliver the Level 1 Data Migration Plan on or before such Approved Date.		

9.2 Data Migration

Z.9.2.1		Mandatory
The Service Provider shall ensure that the proposed Data Migration Strategy allows for continuity of business as usual on the Operational Commencement Date.		

Z.9.2.2		Mandatory
The Service Provider shall ensure that the proposed Data Migration Strategy allows for continuity of business as usual on each Go-Live Date of the Notice Processing Services.		

Z.9.2.3		Mandatory
The Service Provider shall develop and comply with a Level 2 Build and Test Data Migration Plan and shall submit such a plan to TfL for Assurance.		

Z.9.2.4		Mandatory
The Service Provider shall develop and comply with a Level 2 Detailed Plan for Data Migration Execution and shall submit such a plan to TfL for Assurance.		

Z.9.2.5		Mandatory
The Service Provider shall provide TfL with the Data Migration Report in accordance Schedule 3: Milestones and Deliverables.		

Z.9.2.6		Mandatory
The Service Provider shall analyse the Data from the Source System(s), identify data quality issues and provide a Data Quality Report to TfL that details the work required to be completed prior to, during and after data migration.		

Z.9.2.7		Mandatory
The Service Provider shall co-ordinate, execute, and complete Data Cleansing activities prior to the migration of data.		

Z.9.2.8		Mandatory
If the Service Provider fails to migrate any Data to the Service System(s) using the migration process set out in the Data Migration Strategy, it shall submit to TfL a revised Data Migration Strategy for Approval and, when Approved, implement such strategy.		

Z.9.2.9		Mandatory
The Service Provider shall map and migrate to the Service System(s) all Data which (i) is stored on the systems of the relevant Incumbent Service Providers and (ii) is (or may be) required by the Service Provider for the provision of the Services, for example: • all entities defined in the Logical Data Model; • all Reference Data; • User Accounts including passwords;		

- Customer Accounts, Account Holders, Account Users, their identifiers and passwords in clear and/or hashed form including hash key and current hash algorithm;
- MIS Data, excluding data related to CVVC;
- Financial Data, including Payment Data;
- contents of the Document Management System;
- Certificate Authority encryption keys;
- Call recordings;
- Operational Data;
- Evidential Data including images;
- Outbound Correspondence, and
- Inbound Correspondence.

Z.9.2.10		Mandatory
The Service Provider shall transfer all physical Data and records related to the Enforcement Operations from the relevant Incumbent Service Provider.		

Z.9.2.11		Mandatory
The Service Provider shall provide assistance when required to Other Service Providers as instructed by TfL for the migration of Data used in providing other Service Element(s) in accordance with Clause 15.		

Z.9.2.12		Mandatory
The Service Provider shall develop and comply with a proposed set of actions necessary to resolve source data quality issues and shall submit such proposed actions to TfL for Assurance.		

Z.9.2.13		Mandatory
The Service Provider shall create a Data Dictionary during Implementation that contains an entry for each Data item, including without limitation: • Data Structure including without limitation: size, data type, description, validation rules, maximum/minimum values; • Physical location of Data; • Processes that create the Data; • Processes that can edit/delete the Data; • Changes that have amended the format or content of the Data; • Applications that use the Data; and • Owner of the Data.		

Z.9.2.14		Mandatory
The Service Provider shall maintain the Data Dictionary for the Term, this shall include without limitation, amending its contents where required after each change and release to the Service System(s).		

Z.9.2.15		Mandatory
The Service Provider shall supply the Data Dictionary in a human readable format to TfL on request.		

Z.9.2.16		Mandatory
The Service Provider shall identify and document the mapping for each Data item to be migrated from the Source System(s) to the Service System(s).		

Z.9.2.17		Mandatory
The Service Provider shall identify, document and agree any Transformation necessary to migrate a data item.		

Z.9.2.18		Mandatory
The Service Provider shall carry out reconciliation for each Data item being migrated between the Source Systems and the Service System(s) as part of the migration process to ensure Data accuracy, correctness and validity. The Service Provider shall inform TfL of the reconciliation results after each dress rehearsal and again prior to the Implementation of the Service System(s).		

Z.9.2.19		Mandatory
The Service Provider shall ensure that the migrated Data is maintained in accordance with Appendix 11: Data Retention.		

Z.9.2.20		Mandatory
The Service Provider shall upon request by TfL, allow TfL full access to conduct an audit in accordance with Clause 36 (Audit and Inspection), including the following areas: • reconciliation of source to target Data; • the method of report production and any Data transformations; and • queries and conditions used for Data extraction.		

Z.9.2.21		Mandatory
The Service Provider shall maintain documentation of all Data processing operations under the Service Provider's responsibility, which shall be provided to TfL within five (5) days of a request from TfL or such other period as TfL may specify from time to time.		

Z.9.2.22		Mandatory
The Service Provider shall ensure that all in-flight Data processing operations have both their status and stage preserved during migration such that they can continue to be processed by the Service Provider in accordance with Schedule 2 (Statement of Requirements (Business Operations)).		

9.3 Data Integrity

Z.9.3.1		Mandatory
The Service Provider shall provide mechanisms and procedures to allow Data to be reconciled between any Data Stores, and to correct inconsistent and incomplete Data.		

Z.9.3.2		Mandatory
The Service Provider shall perform reconciliation of specific record types between each Service Element and other Solution Elements, with a frequency to be determined by TfL from time to time.		

Z.9.3.3		Mandatory
The Service Provider shall prove referential integrity, consistency and completeness of all replicated Data on request by TfL and at intervals no less than once per week.		

Z.9.3.4		Mandatory
The Service Provider shall ensure that its processes for collecting Personal Data, in any format, comply with Privacy Legislation.		

9.4 Reference Data

Z.9.4.1		Mandatory
The Service Provider shall maintain and manage all Reference Data unless otherwise agreed in writing with TfL.		

Z.9.4.2		Mandatory
The Service Provider shall identify and populate all Reference Data required for Testing in accordance with Schedule 4: Testing Regime.		

Z.9.4.3		Mandatory

The Service Provider shall identify and populate all Reference Data required for the Operational Commencement Date.

Z.9.4.4		Mandatory
The Service Provider shall ensure that only Authorised Users are permitted to undertake changes to Reference Data.		

Z.9.4.5		Mandatory
The Service Provider shall ensure that all Reference Data has valid start and end dates, with the exception of the latest record which may have no end date.		

Z.9.4.6		Mandatory
The Service Provider shall ensure that all modifications to Reference Data records are auditable including, without limitation, recording the Authorised User.		

Z.9.4.7		Mandatory
The Service Provider shall ensure that the audit history of Reference Data maintains versioning of the Reference Data.		

Z.9.4.8		Mandatory
The Service Provider shall request and implement any Changes to Reference Data in accordance with section 9: (Change Control Request Procedure) unless otherwise agreed with TfL.		

10. DOCUMENTATION

This section covers those requirements relating to Documentation. This includes system Documentation and Operational Documentation. Requirements applying to both are contained in the general section. This section should be read in conjunction with Schedule 3: Milestones and Deliverables.

10.1 Documentation

Z.10.1.1		Mandatory
The Service Provider shall develop and comply with procedures for maintenance and support and shall submit such procedures to TfL for Assurance.		

Z.10.1.2		Mandatory
The Service Provider shall develop, review, update and comply with procedures for maintenance and support when Changes are made to the Services, and shall submit such procedures including any updates to TfL for Assurance within 4 weeks of the Change.		

Z.10.1.3		Mandatory
The Service Provider is responsible for identifying all documents, including procedures, impacted by planned and agreed Changes, and notifying TfL of these documents before the Change is agreed with TfL.		

Z.10.1.4		Mandatory
The Service Provider shall ensure all documentation described in Schedule 3: Milestones and Deliverables and Schedule 4: Testing Regime and all other Documentation requested by TfL, is provided to TfL for review as and when modified during the Term.		

Z.10.1.5		Mandatory
The Service Provider shall submit to TfL for Approval, a Review Schedule and, when Approved, comply with such Review Schedule. The Review Schedule shall:		

• allow time for: • TfL reviewers to read the document(s) to be reviewed, including any referenced supporting documentation, and • record and return review comments to the Service Provider; • assuming no less than two (2) revisions of each document; • avoiding the simultaneous release of each document

Z.10.1.6		Mandatory
The Service Provider shall maintain and store all Service System(s) Documentation under Configuration Management.		

Z.10.1.7		Mandatory
The Service Provider shall ensure that the Configuration Management Processes and tools are described in the Quality Plan.		

Z.10.1.8		Mandatory
The Service Provider shall ensure Documentation is provided to TfL in electronic and/or paper format as requested by TfL.		

Z.10.1.9		Mandatory
The Service Provider shall provide electronic copies of Documentation in Microsoft Office (Word, Visio, Excel or PowerPoint) and/or PDF formats as requested by TfL from time to time.		

Z.10.1.10		Mandatory
All electronic Documentation shall be issued to and stored in the Document Library.		

Z.10.1.11		Mandatory

The Service Provider shall ensure that all Service System(s) Documentation is complete such that a Third Party with the requisite technical background could reconstruct the Service System(s) from the Software Source Code and (COTS) components, the operating System Software and the Hardware.

Z.10.1.12		Mandatory
The Service Provider shall ensure that all Documentation is complete for a technician familiar with the technologies to perform all necessary support, maintenance and enhancement tasks for the Hardware and Software making up the Service System(s).		

Z.10.1.13		Mandatory
The Service Provider shall ensure that all Software in the TfL Foreground Materials is fully documented and that promptly following a written request by TfL all such Software and related Documentation is delivered-up to TfL in accordance with Clauses 38.5 and/or 40.1.		

Z.10.1.14		Mandatory
The Service Provider shall ensure that all documentation contained in specialist tools, such as design tools, is provided to TfL in formats accessible from standard TfL documentation tools.		

Z.10.1.15		Mandatory
The Service Provider shall share design and technical Documentation relating to Interfaces with TfL, the Connected Parties, and prospective Connected Parties as specified by TfL. The Service Provider shall ensure that the format and content is agreed with the Connected Party such that the same documentation is used to verify, develop, and test the Interfaces.		

Z.10.1.16		Mandatory
The Service Provider shall ensure documentation for Operational Processes and Procedures is provided for all tasks to be undertaken by the Service Provider from the Operational Commencement Date. This shall, without limitation comprise:		

- procedures for operation of the Services;
- procedures for maintenance and support of the Services and
- references to relevant Service System(s) Documentation.

11. FACILITIES, PERSONNEL, STAFFING & TRAINING

This section lists the requirements related to the provision of facilities, including Security, Maintenance and Post Room facilities. This section also covers requirements for Personnel (both the Service Provider's and TfL's), as well as their recruitment and training.

11.1 Organisation

Z.11.1.1		Mandatory
The Service Provider shall collaborate with Other Service Providers to carry out maintenance and manage the resolution of Incidents.		

Z.11.1.2		Mandatory
The Service Provider shall ensure a support plan is provided which details the support services that will be provided to TfL and to Other Service Providers in accordance with Clause 15.		

Z.11.1.3		Mandatory
The Service Provider shall attend regular meetings with TfL and any related Third Parties upon request from TfL.		

Z.11.1.4		Mandatory
The Service Provider shall ensure that working practices conform to TfL’s commitment to the Investors in People scheme initiative as stated in Appendix 09: IIP Standard.		

Z.11.1.5		Mandatory
The Service Provider shall ensure that its organisation is structured to ensure focus on excellence in customer service and compliance with this Agreement.		

Z.11.1.6		Mandatory

The Service Provider shall ensure that its organisation is structured to enable and promote clear, accurate and regular communications between the Service Provider's Personnel and TfL's Personnel.

Z.11.1.7		Mandatory
The Service Provider shall ensure that person(s) are nominated to be responsible for the delivery of the Services and are contactable by TfL at all times.		

Z.11.1.8		Mandatory
The Service Provider shall ensure that TfL is advised on a rolling weekly basis of the name(s) and contact details of the appointed person(s) responsible for the delivery of the Services and shall ensure that they are available for contact by TfL at all times.		

Z.11.1.9		Mandatory
The Service Provider shall ensure that a permanent on-site operations manager takes overall responsibility for management of the Services. This person is to be the key contact for TfL's Personnel based on the Service Provider's Premises and for the TfL operations and contract management team.		

11.2 Premises

Z.11.2.1		Mandatory
The Service Provider shall ensure that all Premises are provided and managed in accordance with Schedule 18: Premises.		

11.3 Service Provider Recruitment and Staffing

Z.11.3.1		Mandatory
The Service Provider shall ensure that there is a nominated member of the Service Provider's Personnel at all times responsible for ensuring that the Service Provider is		

complying with its obligations under Privacy Legislation and FOI Legislation and in accordance with Appendix 10: Information Governance and Schedule 5: Service Level Agreement.

Z.11.3.2		Mandatory
The Service Provider shall ensure that only appropriately qualified Personnel are employed to provide the support service and Maintenance.		

Z.11.3.3		Mandatory
The Service Provider shall ensure that when a member of the Service Provider's Personnel is dismissed or leaves, all security devices and access cards are returned and the individual is escorted from the Premises immediately.		

Z.11.3.4		Mandatory
The Service Provider shall provide job descriptions for those roles identified by the Service Provider to be necessary for the delivery of Services to TfL for Approval as part of the Detailed Design. At a minimum, this shall include job descriptions for those Key Personnel outlined in Schedule 11: Key Personnel.		

Z.11.3.5		Mandatory
The Service Provider shall provide job descriptions of its Personnel to TfL upon request. Job descriptions must include as a minimum, details of: • key accountabilities; • key competencies; • scope of each role; and • minimum qualifications and experience necessary for the individual to fulfil the role.		

Z.11.3.6		Mandatory

The Service Provider shall provide suitably qualified and trained Personnel to deliver the Services.

Z.11.3.7		Mandatory
The Service Provider shall ensure that the scope of the identified job roles clearly identifies the responsibilities and accountability for outputs and hand-offs.		

Z.11.3.8		Mandatory
The Service Provider shall ensure that TfL is notified immediately of the occurrence of any of the following regarding the Service Provider's Personnel: • suspensions; • disciplinary proceedings; • dismissals; and/or • Key Personnel appointments		

Z.11.3.9		Mandatory
The Service Provider shall ensure that appropriate and relevant Personnel security checks are performed for new Service Provider Personnel prior to the commencement of their employment including, without limitation: • reference checks; • credit checks; • media checks; and • Criminal Records Bureau (CRB) checks. The Service Provider shall submit to TfL for Approval its proposed security checks for new Service Provider Personnel and, when Approved, implement such security checks.		

Z.11.3.10		Mandatory

In the event of the Service Provider's Personnel taking any action that might compromise the position of TfL, the Service Provider shall alert TfL within twenty four (24) hours of the action and provide details of their planned resolution of the action within an appropriate timescale.

Z.11.3.11		Mandatory
TfL reserves the right to request the removal of any of the Service Provider's Personnel from the provision of the Services in accordance with Schedule 11: Key Personnel.		

Z.11.3.12		Mandatory
The Service Provider shall replace Personnel that cease to be employed by the Service Provider with a replacement who has the equivalent or better skills and experience for the role.		

Z.11.3.13		Mandatory
The Service Provider shall replace Personnel moved from their existing role with a replacement that has the equivalent or better skills and experience for the role.		

Z.11.3.14		Mandatory
The Service Provider shall request TfL approval for the replacement of any Key Personnel in accordance with Schedule 11: Key Personnel.		

11.4 Training

Z.11.4.1		Mandatory
The Service Provider shall include, without limitation, a detailed review of the following areas in the induction course referred to in Z 11.5.1: • Privacy Legislation; • FOI Legislation;		

- obligations, codes and procedures for its Personnel;
- Environmental Information Regulations;
- Computer Misuse Act 1990;
- security processes and procedure;
- Premises rules and regulations;
- methods to ensure Personnel have a clear understanding of their duties and hours; and
- methods to ensure Personnel are competent to use all necessary Equipment and Service System(s) in a safe and efficient manner.

11.5 Service Provider Personnel Training

Z.11.5.1		Mandatory
The Service Provider shall submit to TfL for Approval and, when Approved, comply with the contents of and materials to be used for a formal induction course for new Personnel.		

Z.11.5.2		Mandatory
The Service Provider shall ensure that the content of the induction course covers the areas including, but not limited to: • methods to ensure Service Provider Personnel have a clear understanding of their duties and hours; • methods to ensure Service Provider Personnel have a clear understanding of their obligations with regard to Data Protection, the Freedom of Information Act and the Security requirements; and • methods to ensure Service Provider Personnel are competent to use all necessary Equipment and Service System(s) in a safe and efficient manner.		

Z.11.5.3		Mandatory

The Service Provider shall provide ongoing training in accordance with the Training Plan for all Service Provider Personnel required to manage and operate the Service System(s).

Z.11.5.4		Mandatory
The Service Provider shall provide suitably qualified instructors for each of the training courses.		

Z.11.5.5		Mandatory
The Service Provider shall ensure that all Service Provider's Personnel attend a formal induction course provided by the Service Provider in accordance with the Training Plan.		

Z.11.5.6		Mandatory
The Service Provider shall submit to TfL for Approval and, when Approved, comply with a detailed Training Plan for all the Service Provider's Personnel involved in the delivery of the Service System(s) The plan shall cover the following areas, such as but not limited to: • the Service Provider's approach to training; • the Service Provider's proposals for induction training; and • the Service Provider's proposals for periodic refresher training and Personnel development training. The Training Plan shall include any specific training requirements as Approved by TfL.		

Z.11.5.7		Mandatory
The Service Provider shall ensure that an operating procedure for the Premises CCTV operation (the "**CCTV Operating Procedure**") is documented and Approved by TfL.		

Z.11.5.8		Mandatory
The Service Provider shall ensure that all appropriate Personnel are trained on the CCTV Operating Procedure.		

Z.11.5.9		Mandatory
The Service Provider shall provide all necessary induction and on-going training and supporting materials to all its Personnel for any changes made to the Services. For the avoidance of doubt, this shall include, but not be limited to training on the following: • FAQs; • intranet pages; • Operational Users screen guidance; • mail room item tracking and scanning; • Customer service; • Contact Centre guidelines; and • training and materials relevant to the operation of the Services.		

Z.11.5.10		Mandatory
The Service Provider shall submit all training, supporting materials, quality processes and procedures relating to Services to TfL for Approval at least twelve (12) weeks prior to use and, when Approved, comply with such processes and procedures.		

Z.11.5.11		Mandatory
The Service Provider shall train both relevant TfL Personnel and Service Provider Personnel in the same training sessions in respect of any change required as a result of operating the relevant Services.		

Z.11.5.12		Mandatory
The Service Provider shall prepare, deliver and maintain on an on-going basis appropriate training procedures for each of its teams of Personnel as detailed in its proposed organisation structure.		

Z.11.5.13		Mandatory

The Service Provider shall ensure that updated course materials are provided to TfL for the purposes of training TfL Personnel upon request from TfL.

Z.11.5.14		Mandatory
The Service Provider shall ensure that all training manuals and courses are updated to reflect changes to operational practices and lessons learned.		

Z.11.5.15		Mandatory
The Service Provider shall ensure that its Personnel have access to all Documentation appropriate to the performance of any role to which they are assigned.		

Z.11.5.16		Mandatory
The Service Provider shall ensure that Authorised TfL Personnel can attend training sessions facilitated by the Service Provider to ensure the necessary standards of training are implemented on a consistent basis, upon request by TfL.		

Z.11.5.17		Mandatory
The Service Provider shall devise and implement training (including ongoing training, for the Service Provider's Personnel and nominated TfL Personnel) on new technology, where a technology change is necessary for the provision of the relevant Services.		

Z.11.5.18		Mandatory
The Service Provider shall revise training sessions and materials to incorporate updates on any future amendments to applicable Law.		

11.6 TfL Personnel and Training

Z.11.6.1		Mandatory
The Service Provider shall provide training on the MIS to Authorised TfL Personnel as requested by TfL from time to time during the term of the Agreement.		

Z.11.6.2		Mandatory
The Service Provider shall provide training on the MIS to Authorised TfL Personnel on the Service Provider's Premises.		

Z.11.6.3		Mandatory
The Service Provider shall submit to TfL for Approval and, when Approved, comply with a detailed Training Plan for Authorised TfL Personnel including timescales and course outlines.		

Z.11.6.4		Mandatory
The Service Provider shall provide Authorised TfL Personnel with unlimited viewing rights to all Service System(s) and Documents relating to the Services.		

Z.11.6.5		Mandatory

The Service Provider shall ensure that TfL Personnel are trained sufficiently to enable them to effectively and efficiently carry out support activities including, without limitation:

- providing Policy Guidance in response to an escalated query from the Service Provider;
- approving and completing sign-offs required by TfL;
- monitoring feedback actions from weekly meetings with the Service Provider;
- resolving escalated queries from Customer correspondence and complaints;
- providing training to Operational User(s) and team leaders on an ad hoc and scheduled basis;
- providing input to scheduled inductions;
- providing input in the development training courses and materials;
- identifying process improvements; and

• providing guidance to the Service Provider's team managers when implementing new processes.

Z.11.6.6		Mandatory
The Service Provider shall provide training sessions following the employment of new TfL Personnel, at such times requested by TfL.		

12. FINANCE

This section covers those requirements which are additional to those requirements covered in Schedule 2: Statement of Requirements (Finance).

12.1 Unidentified Payments

Z.12.1.1		Mandatory
The Service Provider shall ensure that Unidentified Payments are managed in accordance with Schedule 32: Revenue Collection and Payment.		

Z.12.1.2		Mandatory
The Service Provider shall ensure that the Service System(s) has the functionality to record and store details of Unidentified Payments.		

Z.12.1.3		Mandatory
The Service Provider shall ensure that the Service System(s) has the functionality to search for Unidentified Payments.		

Z.12.1.4		Mandatory
The Service Provider shall ensure that the Service System(s) has the functionality to allocate an Unidentified Payment to a Customer's Account.		

12.2 Fraud Detection

Z.12.2.1		Mandatory
The Service Provider shall provide all required and requested Data and statements directly to the Metropolitan Police Service (or appropriate relevant authority) for the purposes of credit card fraud and other investigations, unless otherwise specifically requested by TfL.		

Z.12.2.2		Mandatory
The Service Provider shall provide any requested Data and statements to the Metropolitan Police Service (or appropriate relevant authority) within the timescales specified by TfL and at no cost to TfL. A log of such events shall be maintained, providing traceability to the Data provided, and this log should be provided to TfL for inspection on request.		

Z.12.2.3		Mandatory
The Service Provider shall ensure that the Service System(s) logs all Data provided to the Metropolitan Police Service.		

12.3 Payment Application Compliance

Z.12.3.1		Mandatory
The Service Provider shall use a payment application to process debit and credit card payments that complies with the PCI DSS Payment Application Data Security Standard (PA-DSS).		

Z.12.3.2		Mandatory
The Service Provider shall ensure the card payment processing application achieves compliance with the PCI DSS Payment Application Data Security Standard (PA-DSS) by the Operational Commencement Date.		

Z.12.3.3		Mandatory
The Service Provider shall provide TfL via a secure method with a monthly report detailing progress towards PCI compliant status until PCI compliant status is achieved.		

Z.12.3.4		Mandatory
The Service Provider shall ensure that PCI compliance is maintained in accordance with the PCI DSS Payment Application Data Security Standard (PA-DSS), as may be amended		

from time to time, at all times during the Operational Phase of this Agreement at no cost to TfL.

Z.12.3.5		Mandatory
The Service Provider shall provide to TfL quarterly scan reports as are required to demonstrate PCI compliance.		

Z.12.3.6		Mandatory
The Service Provider shall conduct monthly vulnerability scans as required by the PCI DSS and send the results via a secure method to the Authorised TfL Personnel.		

Z.12.3.7		Mandatory
The Service Provider shall, after any change to the infrastructure which for the avoidance of doubt includes firewall rule changes, carry out and send the results of the internal vulnerability scans and penetration test via a secure method to Authorised TfL Personnel.		

Z.12.3.8		Mandatory
The Service Provider shall employ the services of a Payment Application-Qualified Security Assessor(s) (PA-QSAs) to ensure all compliant payment processing applications achieves compliance for PCI DSS.		

13. INTERFACES

This section covers those requirements relating to the Interfaces and should be read in conjunction with Appendix 13: Interface Catalogue.

13.1 General

Z.13.1.1		Mandatory
The Service Provider shall provide secure and audited access to Service System(s) from TfL desktop services, to all Service applications, in accordance with Schedule 14: Security.		

Z.13.1.2		Mandatory
The Service Provider shall provide non-production support and technical facilities to test interconnections with all Connected Parties and TfL in accordance with Schedule 4: Testing Regime.		

Z.13.1.3		Mandatory
The Service Provider shall submit to TfL for Approval and, when Approved comply with the Interface Specification Test Strategy.		

Z.13.1.3b		Mandatory
The Service Provider shall design, submit to TfL for Assurance and, when Assured, maintain the Interface Specification.		

Z.13.1.4		Mandatory
The Service Provider shall enable transfer of Data into TfL's Finance System.		

Z.13.1.5		Mandatory
The Service Provider shall enable transfer of Data into TfL's MIS Shared Drive.		

Z.13.1.6		Mandatory

The Service Provider shall provide the Interfaces and network connections in accordance with Appendix 13: Interface Catalogue.

Z.13.1.7		Mandatory
The Service Provider shall operate the Interfaces and network connections to the Service Levels in accordance with Schedule 5: Service Level Agreement.		

Z.13.1.9		Mandatory
The Service Provider shall ensure that the Interface Specification contains, without limitation, the following information for each Service System(s) Interface: • the functional design; • the technical design; • the content of the Data to be exchanged; • the format of the Data to be exchanged; • the static Data which are required to decipher the meaning of the Data exchanged; • the bearer protocols to be used; • any sequencing constraints or assumptions; • error handling measures; • measures to ensure Data integrity; and • any other Information necessary for the Interface to operate correctly.		

Z.13.1.10		Mandatory
The Service Provider shall submit to TfL for Assurance and, when Assured, comply with operator manuals for the Interface Specification.		

Z.13.1.11		Mandatory

The Service Provider shall clarify any assumptions to be made in implementing any Interface within the Interface Specification.

Z.13.1.12		Mandatory
The Service Provider shall notify TfL and Connected Parties in advance of any Planned Downtime of Service System(s) Interfaces. The minimum period of notification shall be five (5) Working Days in advance for Planned Downtime.		

Z.13.1.13		Mandatory
The Service Provider shall ensure that all Planned Downtime of Service System(s) Interfaces is approved in advance in writing by TfL.		

Z.13.1.14		Mandatory
The Service Provider shall request all Changes to the Interface Specification in accordance with the Change Control Request Procedure.		

Z.13.1.15		Mandatory
The Service Provider shall re-use existing Interfaces where possible provided that this has been Assured by TfL.		

Z.13.1.16		Mandatory
The Service Provider shall participate in workshops with TfL, Other Service Providers and/or Third Parties to confirm the Detailed Design of any Service System(s) Interface and any new Interface if requested by TfL.		

Z.13.1.17		Mandatory
The Service Provider shall design, Test and operate all Service System(s) Interfaces and network connections with TfL and Connected Parties on request by TfL in order to operate the Service System(s).		

Z.13.1.18		Mandatory
The Service Provider acknowledges that TfL may, from time to time, require the Service Provider to add additional Service System(s) Interfaces to the Interface Specification in accordance with Schedule 9: Change Control Request Procedure.		

Z.13.1.19		Mandatory
The Service Provider shall issue an updated Interface Specification to all Connected Parties and TfL following any changes to the Interface Specification.		

Z.13.1.20		Mandatory
The Service Provider shall implement the Interfaces to ensure compatibility with prior versions of any defined Interface unless otherwise agreed in writing by the Connected Parties and TfL. The proposed features and functionality of such an Interface must be submitted to TfL, for Assurance prior to being implemented		

Z.13.1.21		Mandatory
The Service Provider shall ensure that all Service System(s) Interfaces are compliant with the Government Digital Services (GDS) Manual (as updated from time to time).		

Z.13.1.22		Mandatory
The Service Provider must design, build, test, and maintain the Service System(s) Interfaces in accordance with Appendix 13 (Interface Catalogue of Schedule 2 (Statement of Requirements (Business Operations)). The Service Provider should use the contents of Section 3 of the Interface Catalogue as indicative information only and must undertake its own design activities.		

14. WEB REQUIREMENTS
This section covers those requirements relating to the Interfaces and interactions between TfL's web facilities and the Services Provider's Service System(s).w
14.1 General

Z.14.1.1		Mandatory
The Service Provider shall produce the following products in collaboration with TfL, in accordance with Schedule 3: Milestones and Deliverables, to be submitted to TfL for Approval : • Web Channels Integration Design including, without limitation, connectivity, security, load balancing, service monitoring, capacity and scalability design, data, technologies; • Business Transactions Design; • Customer Interactions Handler Design – specify all functional processes to handle all Business Transactions and transaction steps; • Customer Web Channels Test Strategy; • Customer Web Channels Test Plan and Test Data; • Customer Web Channels Test Results – include risks & issues and mitigations; and • Customer Web Channels Integration Delivery Plan, including co-ordinations plans, milestones, and key resources details.		

Z.14.1.2		Mandatory
The Service Provider shall ensure that the Service System(s) provide a Service Oriented Architecture (SOA) to enable the customer experience to be built independently of any constraints relating to the Service Provider’s technology and that the customer experience can be built as a discreet and separate entity to the Service System(s).		

Z.14.1.3		Mandatory

The Service Provider shall ensure the Service System(s) adhere to the user interface guide in accordance with Appendix 13: Interface Catalogue.

Z.14.1.4		Mandatory
The Service Provider shall provide the Service System(s) functionality through an Application Programming Interface (API) compliant with the TfL Online Toolkit.		

Z.14.1.4b		Mandatory
The Service Provider shall provide Customer FAQs and answers through an Application Programming Interface (API) which complies with the TfL Online Toolkit.		

Z.14.1.5		Mandatory
The Service Provider shall ensure that the defined and implemented approach to error handling is consistent with the Interface Specification.		

Z.14.1.6		Mandatory
The Service Provider shall ensure that the Service System(s) API is released with a version numbering convention as defined in the TfL Online Toolkit.		

Z.14.1.7		Mandatory
The Service Provider shall provide support for the API during the Term.		

Z.14.1.8		Mandatory
The Service Provider shall ensure that the Service System(s) meets the requirements of Identity Management using the Single Sign On (SSO) model as defined in the TfL Website Toolkit.		

Z.14.1.9		Mandatory

The Service Provider shall ensure that the Service System(s) allows for anonymous User functionality to be supported as defined throughout this Agreement.

Z.14.1.10		Mandatory
The Service Provider shall ensure secure bi-directional authentication and connection management between the Service System(s) API and TfL Website.		

Z.14.1.11		Mandatory
The Service Provider shall be responsible for monitoring and ensuring the performance of the interactions between the Service System(s) API and TfL Website in accordance with Schedule 5: Service Level Agreement.		

Z.14.1.12		Mandatory
The Service Provider shall provide the Service Model to support the web related business activities.		

Z.14.1.13		Mandatory
The Service Provider shall ensure all Data Quality rules are identified, and defined in the Interface Specification.		

Z.14.1.14		Mandatory
The Service Provider shall ensure that the content and references of the Service System(s) API error messages are defined in the Interface Specification.		

Z.14.1.15		Mandatory
The Service Provider shall comply with level 'AA' of the WAI's Web Content Accessibility Guidelines (as updated from time to time).		

Z.14.1.16		Mandatory

The Service Provider shall define a Customer Web Channels Testing Strategy in accordance with Schedule 4: Testing Regime.

Z.14.1.17		Mandatory
The Service Provider shall ensure that Customer input data quality syntax rules are provided to TfL during the Term.		

Z.14.1.18		Mandatory
The Service Provider shall ensure that the Service System(s) accepts 'free text' submissions by Customers from the TfL Website. The Service Provider shall submit to TfL for Approval a proposed limit for characters for free text in accordance with Schedule 3: Milestones and Deliverables and, when Approved, implement such limit.		

Z.14.1.19		Mandatory
The Service Provider shall ensure that the Service System(s) accepts attachments from that the Customer has uploaded to the TfL Website.		

Z.14.1.20		Mandatory
The Service Provider shall ensure that the Service System(s) generates a unique reference number for Communications submitted by a Customer via the TfL Website and this will be displayed to the Customer on the web page.		

Z.14.1.21		Mandatory
The Service Provider shall ensure that the Service System(s) Web Services supports the TfL Business Rules.		

Z.14.1.22		Mandatory
The Service Provider shall ensure that all payments made via the TfL Website are processed in accordance with Schedule 2: Statement of Requirements (Finance) and Schedule 32: Revenue and Collection.		

Z.14.1.23		Mandatory
The Service Provider shall ensure that the Service System(s) provides the time stamping of transactions made through the TfL Website and displays such time stamp to the Customer.		

Z.14.1.24		Mandatory
The Service Provider shall provide Customer facing web pages in order to capture and process any Customer payment related Data.		

Z.14.1.25		Mandatory
The Service Provider shall ensure that the web pages for which it is responsible are viewable to and useable by users of: • PCs; • Macs; and • mobile devices including but not limited to: mobile phones, tablets and netbooks.		

Z.14.1.26		Mandatory
The Service Provider shall ensure that the web pages for which it is responsible are developed and maintained so that they are compatible with legacy, current and future web browsers in use by: • PCs; • Macs; and • Mobile devices including, but not limited to, mobile phones, tablets, and netbooks.		

Z.14.1.27		Mandatory
The Service Provider shall ensure that the web pages for which it is responsible adhere to the latest guidelines as set out in the TfL Online Toolkit published on the TfL Website and updated from time to time.		

Z.14.1.28		Mandatory
The Service Provider shall ensure that payments made against multiple transactions by a single Customer on the TfL Website are summarised and totalled by the Service Provider's payment web pages prior to being submitted by the Customer as a single payment submission.		

Z.14.1.29		Mandatory
The Service Provider shall ensure that individual transactions are independently itemised, traceable and can be automatically presented to TfL in human readable format upon request.		

Z.14.1.30		Mandatory
The Service Provider shall ensure that the payment web pages provide a display of the summary of individual transactions and the grand total to the Customer before payment submission.		

15. EXIT PLANNING

This section covers those requirements relating to the Exit Plan. Additional requirements regarding the Service Provider's Exit Strategy, Exit Plan and Service Transfer Plan are contained within Schedule 16: Exit Plan.

15.1 Exit Planning

Z.15.1.1		Mandatory
The Service Provider shall produce the Exit Plan and Service Transfer Plan for the approval of TfL in accordance with Schedule 3: Milestones and Deliverables and Schedule 16: Exit Plan.		

16. ACCOUNT AGGREGATOR

This section sets out requirements for the Service System(s) to provide to TfL, billing, accounting and transaction information for each Customer, for the purposes of facilitating a single TfL Customer view of all subscribed TfL services. The information will be used by TfL to provide TfL Master Account services.

16.1 Account Aggregator

Z.16.1.1		Mandatory
The Service Provider shall ensure that all financial transactions (including, but not limited to, payments, statements, and refunds) in relation to a Customer's Account are made available to the TfL Website via the Service System(s) API.		

Z.16.1.2		Mandatory
The Service Provider shall ensure that all Data is securely transmitted in accordance with Schedule 14 (Security).		

Z.16.1.3		Mandatory
Not used.		

Z.16.1.4		Mandatory
Not used.		

Z.16.1.5		Mandatory
Not used.		

Z.16.1.6		Mandatory
Not used.		

17. ACCOUNT AUTHENTICATION
TfL require an Authentication and Connection Management Service for LRUC that will be used by Customers to access their account via the Web Interface.
17.1 Account Authentication

Z.17.1.1 (CCR008)		Mandatory
The Service Provider shall ensure that the Operational IT System(s) provides a secure bi-directional Authentication and Connection Management Service between the TfL Website and the relevant elements of the Service Systems.		

Z.17.1.2 (CCR008)		Mandatory
The Service Provider shall ensure that the availability of the Authentication and Connection Management Service is measured and reported on by the Service Provider in accordance with PI 2 (Critical Service Systems and Interface Availability) as detailed in Schedule 5 (Service Level Agreement).		

Z.17.1.3 (CCR008)		Mandatory
The Service Provider shall ensure that the IT Operational System(s) allows Customer Authentication Data to be migrated into the new solution in accordance with Schedule 14 (Security)		

Z.17.1.5 (CCR008)		Mandatory
The Service Provider shall ensure the Operational IT System(s) allows a Customer to log on to the TfL Website by authenticating the Account Users credentials against the following fields: • Account number / customer number		

- Password – passwords must be at least eight characters long and contain a mixture of letters (at least one must be capitalised) and numbers. Existing customer passwords follow the same format required but in the eventuality of a difference in format, will still require supporting.

Z17.1.6 (CCR008)		Mandatory
The Service Provider shall ensure that if a Customers' credentials do not match those held by the Operational IT System(s) then access to an account should be locked after five attempts to log on.		

Z.17.1.7 (CCR008)		Mandatory
The Service Provider shall ensure that the Operational IT System(s) re-directs a Customer to the relevant web pages in order to manage forgotten passwords and/or PINs.		

Z.17.1.8 (CCR008)		Mandatory
The Service Provider shall ensure that the Operational IT System(s) re directs a Customer to the relevant web pages in order to manage password and/or PIN resets		

Z.17.1.9 (CCR008)		Mandatory
The Service Provider shall ensure that the Operational IT System(s) provides a secure and unique login for new Customers registering for an account.		

Z.17.1.10 (CCR008)		Mandatory
The Service Provider shall ensure that the Operational IT System(s) provides a secure and unique log in for Account Users at the point of an Account User being added to an Account.		

Z.17.1.11 (CCR008)		Mandatory
The Serivce Provider shall ensure that the Operational IT Systems(s) provides the functionality to allow a Customer to reset a password and/or PIN by answering a set of security questions as agreed with TfL.		

Z.17.1.12 (CCR008)		Mandatory
The Service Provider shall ensure that the Operational IT Systems(s) provides the functionality to allow a Customers existing security questions to be migrated in to the new solution.		

Z.17.1.13 (CCR008)		Mandatory
The Service Provider shall ensure that the Account Authentication solution is Assured by TfL.		