10.2.3 The Service Provider shall ensure that there are digital backups and other redundancy measures in place to ensure no loss of data owing to system failure.

10.2.4 Wherever possible data shall be anonymised, provided this does not curtail the Authority /the Service Provider's ability to analyse and gain insight from the data.

10.2.5 The Contractor must outline its processes with respect to PCI-DSS compliance in the Operational Manual.

10.2.6 The Contractor must have PCI-DSS Level 1 or 2 accreditation in place, covering all payment channels.

10.3 Data Analysis & Insight

10.3.1 The Service Provider shall, via integration with the Operator's reporting and monitoring suite, provide the Operator with all required data on transaction volumes and types, or customer profiles obtained through the Payment Platform.

11. Cyber Security

11.1 Risk Management

11.1.1 The Service Provider must have risk management policies, procedures, and internal controls in place.

11.1.2 The Service Provider must have an established risk governance framework is in place.

11.1.3 The Service Provider must have a lifecycle approach to cyber risk management program.

11.2 Incident Event and Communications Management

11.2.1 The Service Provider must have procedure in place to respond to a Cyber Security incident, with supporting policies and process documents.

11.2.2 The Service Provider must have an Incident Response Plan detailing actions to be taken in the event of an information security event

11.3 End User Device Security

11.3.1 The Service Provider must have End User Device security policies and procedures, with technical controls to manage end user working remotely within your organisation.

11.4 **Network Security**

11.4.1 The Service Provider must have network security controls and monitoring systems to protect your services, with supporting policies.

11.4.2 The Service Provider must have security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points.

12. **Performance Monitoring & KPIs**

12.1 The table of Key Performance Indicators (KPIs) at 13.7. below quantifies the level of performance required from the Service Provider.

12.2 The Periodic Report (8.2.4.) shall summarise performance against each KPI over the preceding period.

12.3 Any representations made by the Authority following receipt of the Periodic Report must be actioned and implemented by the Service Provider as soon as reasonably practicable.

12.4 The Service Provider must achieve the Minimum KPI Level for every KPI in each calendar month.

12.5 If the Service Provider does not achieve the Minimum KPI Level for any of the KPIs for 3 consecutive the Authority's periods, the Service Provider must pay to the Authority a penalty fee, to be deducted from the Service Provider's next Management Fee payment, as follows:

12.5.1 20% of the Quarter/3 period charges payable to the Authority in respect of the first occasion that the Service Provider fails to achieve the Minimum KPI Level for any KPI for any 3 consecutive Authority periods

12.5.2 30% of the Quarter/3 period charges payable to the Authority in respect of the second occasion that the Service Provider fails to achieve the Minimum KPI Level for any KPI for any 3 consecutive Authority periods

12.5.3 40% of the Quarter/3 period charges payable to the Authority in respect of the third occasion that the Service Provider fails to achieve the Minimum KPI Level for any KPI for any 3 consecutive Authority periods

12.6 If the Service Provider a) fails to achieve the Minimum KPI Level for any KPI for 6 consecutive Authority periods, or b) fails to achieve the Minimum KPI Level for any KPI for 6 or more non-consecutive the Authority periods in a 9 period timeframe, the Authority may terminate the Contract with immediate effect by formal notice.

12.7 Details of KPIs are provided below:

KPI Ref	Description	Minimum KPI Level
A1	System Availability	99%
A2	All agreed revenue collection processes followed	100%
A3	Revenue transferred to the Authority in line with agreed schedule	100%
A4	All agreed actions taken to minimise loss of revenue	90%
B1	Client facing contact (account manager or similar) to be available 24/7	95%
B2	Customer support available during operational hours	95%
C1	All agreed data provided to the Authority /Operator promptly	100%
C2	DPA 2018/UK GDPR processes adhered to and risk of data breach minimised	100%
C3	All third party data integration functions properly	100%
D1	Client help line available to the Authority /Operator 24/7	100%
D2	All reports delivered within required timescales	100%
D3	Required personnel attend scheduled meetings	100%
D4	All actions completed within agreed timescales	100%

SCHEDULE 4 – CHARGES

1. Introduction

1.1 This Schedule 4 sets out the Charges for the delivery of the Services by the Service Provider, and the performance of the Service Provider's other obligations, under or in connection with this Contract.

1.2 The Charges shall be inclusive of all costs and expenses of whatsoever nature and howsoever incurred by the Service Provider in the provision of the Services and the performance of the Service Provider's obligations in accordance with this Contract.

2. Definitions

In this Schedule 4, the following definitions shall have the following meanings:

"**Mobilisation Charges**" means the charges as set out in Clause 4 of this Schedule 4;

"**Parking Payments**" means the payments made by a Customer to pay for parking at a Car Park during the Term that is processed via the Payment Platform but excluding:

(a) any payments which fail or are rejected;

(b) rejected payments; and

(c) payments of penalty charge notices.

"**Payment Period**" means each successive 4 week period in each Year;

"**Rental Charges**" means the charges for rental of a telecommunications line for Car Parks with ANPR installed;

"**SMS Confirmation Revenue**" means the payments made by a Customer to receive additional messaging about the duration of their use of a Parking Space;

"**SMS Reminder Revenue**" means the payments made by a Customer to receive additional messaging about the upcoming expiry of their Parking Payment for use of a Parking Space at a rate [redacted];

"**Transaction Charges**" means [redacted] of Parking Payments made during the relevant Payment Period;

"**Year**" means a twelve (12) month period beginning on the Service Commencement Date and each subsequent successive twelve (12) month period.

3. **Charges**

3.1 Subject to Paragraph 3.4, the Service Provider shall with effect from the Services Commencement Date raise invoices in arrears at the end each Payment Period for the Charges that relate to that Payment Period, and the Authority shall pay the Charges in accordance with this Contract.

3.2 The Charges for each Payment Period is the total Transaction Charges and the such Rental Charges as may be applicable for that Payment Period.

3.3 The Transaction Charges for each Payment Period shall not be fixed but shall be dependent on the level of usage of Parking Spaces by Customers. The Service Provider acknowledges and agrees that the Transaction Charges for each Payment Period may vary.

3.4 The Charges for each Payment Period shall be reduced by the following (to the extent applicable):

3.4.1 deductions for failure by the Service Provider to supply the Services in accordance with the KPIs, calculated in accordance with Schedule 3 (*Specification*); and

3.4.2 any other deductions due in accordance with this Contract (including any overpayments made by the Authority to the Service Provider).

3.5 Any changes to the Charges (save as described in paragraph 3.4) shall only be considered and implemented in accordance with Clause 47 (*Contract Variation*) and Schedule 6 (*Form of Variation*).

3.6 Unless otherwise agreed between the Parties in writing in accordance with paragraph 3.5, [redacted]

4. **Mobilisation Charges**

4.1 [redacted]

5. **Management**

5.1 [redacted] for the following items provided by the Service Provider under the Contract:

(a) management of the Payment Platform;

(b) marketing in relation to the Car Parks of the Payment Platform;

(c) signage in the Car Parks;

(d) Customer surveys regarding use of the Payment Platform; and

(e) SMS messaging to Customers if Customers opt-in for the same.

6. SMS Messaging

6.1 The Service Provider shall be entitled to retain all SMS Confirmation Revenue under this Contract.

6.2 The Service Provider shall pay to the Authority for each Payment Period in arrears all SMS Reminder Revenue under this Contract.

7. Rental Charges

7.1 For such time as the Service Provider provides a telecommunications line for Car Parks with ANPR installed (pursuant to paragraph 1.4 of Schedule 3) the R[redacted]

The Rental Charges shall not be applicable from such time as the Authority notifies the Service Provider pursuant to paragraph 1.4 of Schedule 3 that the Service Provider is no longer required to provide such telecommunications line.

SCHEDULE 5 - PROJECT PLAN

Updated Project Plan to be provided by the Service Provider within 14 days of the Contract Commencement Date.

SCHEDULE 6 - FORM OF VARIATION

PART A

Contract Parties: [*to be inserted*]

Contract Number: [*to be inserted*]

Variation Number: [*to be inserted*]

Authority Contact Telephone: [*to be inserted*]

Date: [*to be inserted*]

AUTHORITY FOR VARIATION TO CONTRACT (AVC)

Pursuant to Clause 47 (Contract Variation) of the Contract, authority is given for the variation to the Services and the Charges as detailed below. The duplicate copy of this form must be signed by or on behalf of the Service Provider and returned to the Procurement Manager as an acceptance by the Service Provider of the variation shown below.

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

....

For the Authority (signed) (print name)

ACCEPTANCE BY THE SERVICE PROVIDER	
Date	**Signed**

PART B – SUPPLY CHAIN FINANCE OPTION RELATED VARIATIONS

1. The Authority is developing a scheme and system whereby the Service Provider may be permitted, at the Authority's sole discretion, to seek payment of invoices in respect of Charges under this Contract within a time period less than the thirty (30) days of receipt set out Clause 11.4.1 (Payment Procedures and Approvals) in consideration for a reduction in the Charges due thereunder (the "**Supply Chain Finance Option**").

2. The Service Provider hereby agrees that where such requests are made by the Service Provider and approved by the Authority, by way of such process and/or systems put in place by the Authority acting either on its own behalf or by or via its employees, agents, contractors or otherwise such request, approval and resulting accelerated and reduced payment shall constitute the Service Provider's exercise of the Supply Chain Finance Option and the valid and legally binding:

2.1 variation by the Parties of the related Charges due and payable to the Service Provider under this Contract; and

2.2 waiver by the Service Provider of any right held previously by it to invoice for and be paid the amount by which the Charges are reduced pursuant to its exercise of the Supply Chain Finance Option.

SCHEDULE 7 - CONTRACT QUALITY, ENVIRONMENTAL & SAFETY CONSIDERATIONS

NOT USED

SCHEDULE 8 – EXIT

1. DEFINITIONS

1.1 In this Schedule 8, the following definitions shall apply:

Exit Assistance	the services and obligations of the Service Provider in the event of expiry or termination of this Contract, as detailed in Schedule 8 (Exit);
Exit Assistance Period	the period starting one hundred and twenty (120) days before the date of expiry or termination of the Contract until the later of: (a) twelve (12) months after the date of expiry or termination in whole or part (as applicable); or (b) completion of all of the Service Provider's obligations under the Exit Strategy;
Exit Data	any data in respect of the performance or operation of the Services.

2. THE EXIT STRATEGY

2.1 The Service Provider shall, within six (6) months after the Contract Commencement Date, deliver a draft Exit Strategy to the Authority which sets out the Service Provider's proposed methodology for achieving an orderly transition of the Services from the Service Provider to the Replacement Service Provider on the expiry or termination of the Contract and which complies with the requirements set out in paragraph 2.7 below. Within twenty (20) Business Days after the submission of the draft Exit Strategy, the Parties will use reasonable endeavours to agree the contents of the Exit Strategy. If the Parties are unable to agree the Exit Strategy then the dispute shall be resolved in accordance with Clause 38 (Dispute Resolution).

2.2 Any failure to agree an Exit Strategy shall not prejudice the rights or remedies of the Authority pursuant to this Schedule 8. If the Service Provider fails to produce an Exit Strategy in accordance with this Schedule 8, then the Authority may produce an Exit Strategy and the Service Provider shall be responsible for the reasonable costs incurred by the Authority in doing this. the Service Provider shall be bound to comply with the terms of such Exit Strategy.

2.3 This Schedule 8 sets out the principles of the exit and Service transfer arrangements that are intended to achieve such orderly transition and shall form the basis of the Exit Strategy.

2.4 The Exit Strategy shall be reviewed and, where appropriate, updated at least once every twelve (12) months and whenever there is any change to the Services.

2.5 At least twenty (20) Business Days before the date of expiry or termination of the Contract, the Parties shall begin a review of the Exit Strategy to ensure that it reflects the circumstances at the time and it shall be the responsibility of the Service Provider to ensure that it does. On request from the Authority, at any time during the Exit Assistance Period, the Service Provider shall make such amendments to the Exit Strategy as required to align the Exit Strategy with the Replacement Service Provider's transition plan as reasonably required by the Authority.

2.6 The Exit Strategy shall be in a form as requested by the Authority and shall include as a minimum (unless required otherwise by the Authority):

2.6.1 address each of the issues set out in this Schedule 8 to facilitate the transition of the Services from the Service Provider to the Replacement Service Provider (with the aim of ensuring that there is no disruption to or degradation of the Services during the Exit Assistance Period);

2.6.2 the management structure to be employed during both transfer and cessation of the Services;

2.6.3 identify critical issues for providing the Exit Assistance;

2.6.4 set out any Authority responsibilities, dependencies on the Authority or Replacement Service Provider;

2.6.5 provision of an inventory of the Exit Data in the Service Provider's possession or control and details on the mechanism for secure transfer of Exit Data in a commonly machine readable form which retains the integrity of the data;

2.6.6 all information reasonably requested by the Authority or the potential Replacement Service Provider relating to the Services and the Service Provider's Personnel that carry out the Services under this Contract;

2.6.7 information regarding daily work volumes for all of the Services for a period of twelve (12) months or where this period does not reflect the true ongoing trends in work volumes, for such longer period as requested by the Authority;

2.6.8 details of work in progress and/or unfinished activities under the Contract at point of request and monthly updates on these throughout the Exit Assistance Period;

2.6.9 provision of such information on hardware, software, processes and procedures as is reasonably required by the Authority to enable discussions with a potential Replacement Service Provider;

2.6.10 any further information requested by the Authority or from a potential Replacement Service Provider as part of initial due diligence;

2.6.11 such co-operation with potential Replacement Service Providers as the Authority reasonably requests.

2.6.12 set out such other details as the Authority considers reasonably appropriate and necessary; and

2.6.13 be updated to incorporate the agreed transition requirements of any Replacement Service Provider to include a detailed description of both the cessation process and how the Services will transfer to the Replacement Service Provider, the documentation, data transfer, (including Exit Data) and security (where applicable) together with a timetable.

2.7 Each Party shall act and negotiate reasonably in agreeing the contents of the Exit Strategy and shall not unreasonably require the exclusion of matters which the other Party reasonably requests should be included or the inclusion of matters which the other party reasonably requests should be excluded.

2.8 The Service Provider and the Authority shall each have the rights and obligations assigned to them in the Exit Strategy, once agreed.

2.9 The Service Provider shall provide Exit Assistance at no additional cost to the Authority.

3. OBLIGATIONS DURING THE EXIT ASSISTANCE PERIOD

3.1 During the Exit Assistance Period, the Service Provider shall provide to the Authority and the Replacement Service Provider or a potential Replacement Service Provider the following assistance, services, material and information set out in the Exit Strategy in order to facilitate the preparation by the Authority of any invitation to tender and/or to reasonably assist and inform any potential Replacement Service Provider undertaking due diligence and/or to assist the Authority with the exit from the Agreement.

3.2 The Service Provider shall ensure that it retains the necessary resources to enable the Service Provider to comply with the requirements set out in this Schedule 8.

3.3 Exit Assistance is subject to the provisions of Clause 36 (Confidentiality and Announcements).

3.4 The Service Provider shall provide reasonable access to its relevant premises and personnel for any potential Replacement Service Provider selected by the Authority so that such potential Replacement Service Provider can undertake the necessary due diligence on provision of the Services to enable it to formulate and cost its Replacement Service offering for the Authority.

3.5 The Service Provider shall provide assistance in the transition of the Services to the Replacement Service Provider, as may be reasonably necessary to enable a smooth transition to take place, assistance to include as a minimum:

3.5.1 ensuring a complete and effective handover of all Services to the Replacement Service Provider, including full details of any work in progress being handed over at the end of the Exit Assistance Period together with applicable status updates, details of all actions carried out to date in respect of such work in progress, when the activity started, its completion date, whether any Service Level applies and any communications history with the Authority regarding the work in progress;

3.5.2 providing reasonable access for the Replacement Service Provider's personnel to the Service Provider's premises and to the extent it is reasonably able to do so its subcontractors' premises during normal Working Hours during the Exit Assistance Period for the purpose of familiarisation of the delivery of the Services and knowledge transfer; providing reasonable access for the Replacement Service Provider's personnel to such members of the Service Provider's Personnel as have been engaged in the provision or management of the Services and who are still employed or engaged by the Service Provider or its subcontractors to facilitate knowledge transfer, including all Key Personnel;

3.5.3 without prejudice to the generality of paragraphs 3.53.5.1 and 3.53.5.2, facilitating the transfer of knowledge to the Replacement Service Provider by providing:

3.5.3.1 a detailed explanation of procedures and operations used to provide the Services in accordance with any operations manual, together with copies of up to date relevant documentation; and

3.5.3.2 details which show where the procedures, processes and work instructions being followed are documented in the operations manual.

3.5.4 providing training (including at any Replacement Service Provider's location where requested), one-on-one job familiarisation and work shadowing to the Replacement Service Provider's personnel. Work shadowing comprises a Replacement Service Provider personnel sitting side-by-side with a Service Provider's Personnel performing an equivalent role in respect of the relevant Services, at the location from which the Service Provider has been delivering the Services, in order to:

3.5.4.1 gain an understanding of how the Service Provider's Personnel performs the tasks and activities associated with their role; and

3.5.4.2 have the opportunity to execute tasks and activities which are the subject of the work shadowing, with close supervision by the Service Provider. The Service Provider shall have the right to stop the Replacement Service Provider's personnel carrying out any such activity if the actions of the Replacement Service Provider's personnel would have an adverse impact on delivery of the Services;

3.5.5 providing such access to the Service Provider's technical support personnel as may be reasonably necessary to resolve any technical problems during the migration of the Services to the Replacement Service Provider;

3.5.6 securely providing copies of the Exit Data, the Authority Intellectual Property Rights on suitable magnetic, optical or other industry standard portable storage media as agreed in the Exit Strategy;

3.5.7 permitting access to the Authority, for itself and any persons acting on its behalf, to the Service Provider's premises and to the extent it is reasonably able to do so its subcontractors' premises during normal Working Hours during the Exit Assistance Period for the purpose of removing any Exit Data or Authority Intellectual Property Rights or for arranging for the migration of the Services to another system.

4. CONTINUATION OF THE SERVICES

4.1 During the Exit Assistance Period the Service Provider shall provide and charge for the Services (to the extent required by the Authority) until there has been a full transitioning of the Services to the Replacement Service Provider to the Authority's reasonable satisfaction.

4.2 Any applicable costs, reasonably incurred in providing Exit Assistance will be charged to the Authority by the Service Provider in accordance with the provisions set out in this Contract. For the avoidance of doubt, the Service Provider shall not be entitled to make any additional charge for any Exit Assistance where the information or activities involved are required in the course of delivering the Services.

4.3 The Parties acknowledge that the migration of the Services from the Service Provider to the Replacement Service Provider may be phased over an agreed period, such that certain of the Services are handed over before others. Where applicable, the Charges for provision of the Services during the Exit Assistance Period shall be pro-rated.

4.4 During the Exit Assistance Period, Services will be provided at no detriment to the Service Levels and in accordance with the Contract.

5. TERMINATION OBLIGATIONS

5.1 The Authority may terminate Exit Assistance (and provision of any continued Services) during the Exit Assistance Period on giving the Service Provider no less than ten (10) Business Days' written notice.

5.2 At the end of the Exit Assistance Period (or earlier if this does not adversely affect the Service Provider's performance of the Services and Exit Assistance and its compliance with the other provisions of this Schedule 8), the Service Provider will (to the extent not already done):

5.2.1 permanently and securely erase any software containing any Exit Data or Authority Data, from any computers, storage devices and storage media that are to be retained by the Service Provider after the end of the Exit Assistance Period subject to its obligations under any provisions in the Contract dealing with audit, records and reporting and to any requirements under Applicable Law;

5.2.2 return to the Authority such of the following as is in the Service Provider's possession or control:

5.2.2.1 all copies of the Authority Intellectual Property Rights and any other software licensed by the Authority to the Service Provider under this Contract; and

5.2.2.2 all materials created by the Service Provider under this Contract, the Intellectual Property Rights in which are owned by the Authority.

5.3 The Service Provider shall comply with its obligations under Clause 36 (Confidentiality and Announcements) and will return to the Authority all Confidential Information and will certify that it does not retain the Authority's Confidential Information save to the extent (and for the limited period) that such information needs to be retained by the Service Provider for the purposes of providing or receiving any Services or Exit Assistance, or complying with any Applicable Law.

5.4 Except where this Contract expressly provides otherwise, all licences, leases and authorisations granted by the Authority to the Service Provider, or the Service Provider to the Authority, in relation to the Services shall be terminated with effect from the end of the Exit Assistance Period.

SCHEDULE 9 – CYBER SECURITY

The Authority is committed to maintaining the confidentiality, integrity and availability of all data it accesses, processes or stores. Where services have been contracted to a third-party to access Authority Data or develop code and/or systems for the Authority, the Service Provider must ensure that Authority Data and products supplied are subject to the standards laid out in this Contract.

1. The Service Provider shall ensure that in relation to the provision of Services, the following are protected to ensure confidentiality, integrity and availability:

   1.1.1 Authority Confidential Data (including Authority Personal Data);

   1.1.2 Authority Restricted Data (being data about any customers, employees, or cardholders);

   1.1.3 Authority Management Restricted Data;

   1.1.4 All information relating to Authority customers, partners and employees;

   1.1.5 Any other information used in the provision of the Services;

   1.1.6 the Authority and the Service Provider's IT and communications systems that process, store or transmit information;

   1.1.7 computer program code used to process Authority Data;

   together referred to in this Schedule 9 as "**Authority Data**".

2. The Service Provider must be able to clearly identify:

   2.1.1 what information systems are used to support the Services;

   2.1.2 which information systems store Authority Data or program code;

   together referred to in this Schedule 9 as "**Service Provider Systems**".

3. The Service Provider will comply with the ISO 27001 or Good Industry Practice relating to data security and protection.

4. The Service Provider undertakes that it shall comply with the provisions of all Data Protection Laws in connection with its processing of Authority Data. The Data Protection Laws shall mean (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR") and any national implementing laws, regulations and secondary legislation, as amended from time to time, in the United Kingdom and; (ii) any successor legislation to GDPR or the Data Protection Act 2018.

5. The Service Provider undertakes that it shall comply with the requirements of the most current published version of the Payment Card Industry Data Security Standard (PCI –DSS) when processing, storing or transmitting card-holder data. The Service Provider will provide the Authority with an annual

letter of attestation from a Qualified Security Assessor (QSA) confirming compliance with PCI –DSS.

6. A member of the Service Provider's Personnel will be appointed to act as Security Point of Contact ("**SPOC**") .This person shall be knowledgeable on information security matters, and be able to respond to the Authority's inquiries regarding information security. This person will also maintain contact with an authority which allows for the tracking of industry best practice for information security matters to understand the current threats posed to Authority Data. This person shall ensure the Service Provider's compliance with its information security obligations under this Contract; and in relation to the Services provided.

Right of Inspection

1. The Authority may, upon giving at least 4 weeks written notice, conduct a security audit of any site or component being used by, or required to be used by, the Service Provider to provide the Services. The Authority shall carry out the audit in such a way to cause as little disruption as reasonably possible to the Service Provider and performance of the Services provided.

2. The Service Provider shall provide all assistance reasonably requested by the Authority in relation to any audit and shall ensure that agreements with any third-party service providers or sub-contractors, shall contain provisions for such an audit.

3. The Service Provider will remediate any points that are identified in the audit by the Authority as being of a risk to Authority Data, or supporting IT Systems and program code.

Awareness and Training

1. The Service Provider shall provide all Service Provider's Personnel who have access to Authority Data or develop products for the Authority, with clear roles and responsibilities pertaining to information security and data protection.

2. The Service Provider shall provide Service Provider's Personnel with specific information security training detailing good security practices on at least an annual basis. This training will reflect current, best industry practices and make Service Provider's Personnel aware of current threat trends.

Information Security Policy and Governance

1. The Service Provider shall ensure that the subject of information security and its importance to the Service Provider's business is represented at a senior level within the Service Provider's organisation and that a formal strategy for information security management has been approved by senior management.

2. A comprehensive, documented and approved set of information security policies will be maintained. These policies must be communicated to the Supplier's personnel, contractors and all their third-parties with access to TFL Data or the Supplier's information systems. These policies must be defined

and approved by management and published and enforced across the organisation. These policies must be reviewed on at least an annual basis or - when a significant change has occurred that necessitates the modification of policy. The Supplier shall ensure that there is a formal disciplinary process for breaches of policy.

3. A data classification methodology that applies throughout the Service Provider's business must be in place. The methodology shall be based on the criticality and sensitivity of the data and systems in use.

4. The Service Provider must maintain a record of categories of processing categories carried out on the Supplier systems to include:

   4.1.1 The name and contact details of the Authority contact who determines the purposes and means of processing Authority Personal Data to the Service Provider;

   4.1.2 The categories of processing of Authority Data carried out on behalf of the Authority.

5. The Service Provider shall have access to specialist information security advice and guidance.

6. The Service Provider must include information in all projects the Service Provider undertakes. For any project, information security objectives must be detailed as part of the overall project. The Service Provider conduct a risk assessment before the project commences in order to identify any risks. Where risks are identified they must be managed by the Service Provider.

7. The Service Provider shall ensure that no Authority Data is stored or transferred via removable data storage media (including laptop computers, smart phones, portable disk drives, magnetic tapes, memory sticks, and CDs).

Third Party Management

1. Services required by the Service Provider's Third-Party service providers shall only be obtained from organisations capable of providing security controls no less rigorous than those the Supplier themselves are required to comply with pursuant to this agreement. Such additional services shall be provided under appropriate contracts.

2. The Service Provider shall have and maintain a Third-Party Assurance Policy, which covers information security. This must be documented, approved, communicated and be enforced across the organisation. The Third-Party Assurance Policy must be implemented via a risk based due diligence process whereby potential risks can be identified, communicated to the sub-contractor and managed. The Service Provider shall promptly notify the Authority in writing of any significant risks identified in the due diligence process.

3. Where Authority Data is to be transferred to a Third Party to the Service Provider, the Service Provider shall obtain the prior written authorisation for

the transfer detailing the purpose of the transfer and providing evidence that the Service Provider's Third-Party Assurance Policy has been followed.

4. The Service Provider shall maintain a written record of the processing activities carried out on behalf of the Service Provider by a Third Party.

Human Resource Security

1. The Service Provider shall ensure that a Human Resource Policy is maintained. This policy must be formally documented, approved by management, communicated to all Service Provider's Personnel and contractors and be enforced across the organisation.

2. The policy must ensure that Service Provider's Personnel and contractors understand their responsibilities with respect to information security and data protection.

3. The Service Provider shall clearly define appropriate information security related roles and responsibilities for Service Provider's Personnel, including the limitations of each role and the level of training required.

4. All Service Provider's Personnel and contractors who will be granted access to Authority Data will be subject to background verification checks. This shall be done in compliance with legal regulations and in proportion to the Authority's classification of data to be accessed.

5. The Service Provider must ensure that all Service Provider's Personnel and contractors who have access to Authority Data are:

    5.1.1 Provided information security and data protection awareness and training. As a minimum this must be conducted annually. The awareness and training must be tailored to meet the needs of various employees and their roles;

    5.1.2 Conform to the terms and conditions relating to information security and data protection described in the terms and condition in their employment contracts.

6. On the termination of employment of a Service Provider's Personnel or a contractor the Service Provider must ensure that a process is followed that ensures that all access to Authority Data is removed.

Secure Configuration

1. All external connections to the Service Provider's networks and applications shall be individually identified, verified, and approved by the Service Provider in accordance with the Service Provider's information security policy.

2. All network traffic from external sources must be routed through a firewall before being allowed access to the Service Provider's network. Firewalls must ensure secure connections between internal and external systems and shall be configured so that only required traffic is allowed to pass through.

3. Wireless access to the Service Provider's information systems must be subject to authorisation, authentication, and encryption protocols consistent with security industry best practice, and shall only be permitted from locations approved by the Service Provider.

4. The Service Provider will ensure that its computers and network devices should be securely configured, in particular that:

   4.1.1 Unnecessary user accounts will be removed or disabled;

   4.1.2 Any default password for a user account must be changed to a unique, strong password;

   4.1.3 Unnecessary software will be removed or disabled;

   4.1.4 A personal firewall (or equivalent) must be enabled on desktop PCs and laptops and configured to disable unapproved connections by default.

Information Asset Management

1. The Service Provider shall ensure that a formal process exists to identify and manage information systems that will be used to access, store or process Authority Data.

2. A policy which supports the appropriate use of information systems must be maintained by the Service Provider. This policy must be formally documented, approved by management, communicated to all Service Provider's Personnel and contractors and be enforced across the organisation.

3. The Service Provider shall appoint an owner, who shall be accountable for each information system (the "**Information System Owner**"). This accountability should be documented and formally agreed. The Information System Owner shall have sufficient seniority for the classification of data to be processed on the asset.

4. The Service Provider shall ensure that all information systems that support the Services and Authority Data are maintained on an inventory maintained by the Service Provider. The inventory must be accurate, up to date and contain:

   4.1.1 Type of system;

   4.1.2 Its location;

   4.1.3 Who the Information System Owner is;

   4.1.4 The classification of data that will be processed on the asset.

5. The Service Provider must maintain a policy or process for the handling of information systems and data. This must include:

   5.1.1 where hardware or storage media are required to be destroyed the Service Provider must ensure that this is done in a way that renders any data unrecoverable. The Service Provider must obtain proof of the secure destruction and certify the same;

   5.1.2 where hardware or storage media are to be recycled the Service Provider shall ensure that any data held on the asset is purged to a standard that ensures that all data is un-recoverable.

Access Control

1. The Service Provider shall ensure that an Access Control Policy, as approved by the Authority, is communicated to all Service Provider's Personnel and contractors and is enforced across the organisation. This policy must be based on the principles of lowest levels of privilege and on a 'need to know' basis.

2. The Service Provider must restrict any access to Authority Data to Service Provider's Personnel and contractors who need to access the data only for a legitimate business reason.

3. Access authorisation must be approved by Information System Owner.

4. For each system storing or processing Authority Data:

   4.1.1 Access must be via a user account, (user ID) allocated to each individual employee;

   4.1.2 A formal process must be in place covering:

      4.1.2.1 Provisioning access.

      4.1.2.2 Reviewing access rights on a regular basis;

      4.1.2.3 Ensuring that when an employee or contractor leaves the organisation, or no longer requires access to Authority Data, that their access is removed immediately;

      4.1.2.4 Ensuring that dormant accounts are deactivated after 90 days.

5. The Service Provider will ensure that the systems that will process or host Authority Data provide the following security measures:

   5.1.1 Authentication credentials of the previous user must not appear on the logon prompt or anywhere else that is visible;

   5.1.2 The system must restrict the number of unsuccessful sign-on attempts to prevent password guessing attacks;

5.1.3 Re-authentication of users must occur after session timeout or interruption;

5.1.4 Access to systems shall not be attempted except through authorised user accounts;

5.1.5 Access to systems and services shall be on the basis of job role requirements and authorised by the appropriate manager;

5.1.6 The Service Provider shall ensure that the Service Provider Systems adequately provides the following password management controls:

5.1.6.1 It must not be possible to bypass authentication mechanisms to gain unauthorised access to systems;

5.1.6.2 Authentication data such as passwords must be stored using industry standard one-way cryptographic hashing functions;

5.1.6.3 Password complexity that includes a combination of character types and minimum length that is sufficient to reduce the risk of brute force or dictionary attacks.

6. A privileged user is a user who has been allocated powers or rights within the computer system, which are significantly greater than those available to the majority of users. These include changing system configuration, the ability to add or delete other user accounts or with access to all or most of the data in the system. Where the Service Provider needs to authorise an account that has privileged access on any system that stores or processes Authority Data the following must be adhered to:

6.1.1 A record of all access requests and changes related to privileged accounts must be maintained and the access changes must be documented;

6.1.2 Privileged accounts must not be used for day to day activities such as email and internet access;

6.1.3 Privileged accounts that have not been used for thirty days must be disabled or removed;

6.1.4 Use of privileged user access by developers in production environments must be restricted to planned or emergency change support.

Encryption

1. The Service Provider must ensure that Authority Data that contains Authority Personal Data is encrypted:

1.1.1 When being transferred across computer and telecommunications networks;