SCHEDULE 14

Security

1. **Scope**

1.1 This Schedule sets out the Service Provider's obligations in respect of:

(A) TfL's security requirements relating to the System and the provision of Services;

(B) the development, updating and testing of the Security Policy and Security Plan.

2. **Legislation, Standards and Working Practice**

2.1 The Service Provider shall adhere to the legislation set out in Table 1 below; as such legislation may be amended or superseded by equivalent standards from time to time.

Table 1 - Legislation
• Data Protection Act 1998 • Privacy and Electronic Communications Regulations 2003 • Human Rights Act 1998 • Civil Traffic Enforcement Approved Devices

2.2 The Service Provider shall adhere to the standards and working practices set out in Table 2 below, as such Legislation may be amended or superseded by equivalent standards from time to time.

Table 2 – Standards and Working Practices
• **TfL Information Security Controls Framework (ISCF)** for IT security and Service Management of TfL Services (Annex 1 to this Schedule) • **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) • **BS10012**:**2009** is the British standard that specifies the requirements for a Personal Information Management System (PIMS) to aid compliance with the Data Protection Act (DPA). • **ICO Guide to Data Protection Audits** guidance from the Information Commissioner's Office • **ICO CCTV Code of Practice** • **Centre for the Protection of National Infrastructure 10 Steps to**

Cybersecurity;

3. **Security Policy**

3.1 The Service Provider shall ensure that a Security Policy which meets the requirements of this paragraph 3 (the "**Security Policy**") is initially Approved in accordance with the Implementation Plan and the Service Provider shall subsequently, at its own cost and in accordance with the requirements:

(A) refine, expand and amend the Security Policy:

(1) in accordance with the Implementation Plan (and, in any event, prior to the Operational Commencement Date); and

(2) within ten (10) Business Days, or such other period as may be expressly agreed in writing by the Parties following the implementation of a Change so as to incorporate the effects of that Change into the Security Policy (where applicable); and

(B) promptly prepare a written review of the Security Policy (as the same may be amended from time to time in accordance with paragraph 3.1(A)(2)) upon request from TfL and in any event at least once in every twelve (12) month period following the Operational Commencement Date.

In each case, the Service Provider shall submit a copy of the Security Policy and the review provided pursuant to paragraph 3.1(B) (as applicable) to TfL for Approval.

3.2 The Service Provider shall ensure that the Security Policy shall:

(A) include specific detail related to the Services and the System;

(B) reference and comply with, and be consistent with, this Schedule 14;

(C) reference and comply with the security requirements set out in Schedule 2 (*Statement of Requirements*);

(D) comply with:

(1) the TfL Information Security Classification Standard set forth in Schedule 34 (*TfL Policies*);

(2) the TfL Information Security Controls Framework (ISCF), (Annex 1 to this Schedule 14);

(3) the TfL security requirements in accordance with this Schedule 14;

(4) TfL's security requirements while on both TfL's and the Service Provider's Premises in accordance with this Schedule 14; and

(E) comply with such other requirements that TfL may reasonably request from time to time.

3.3 The Service Provider's Security Policy shall be set out in Annex 2 (*Security Policy*) to this Schedule 14.

3.4 The Service Provider shall ensure that it is able to promptly provide TfL with the current version of the Security Policy on request.

3.5 Unless and until the Service Provider's Security Plan has been Approved in accordance with paragraph 4 below, the Service Provider shall comply with Service Provider's Security Policy.

4. **Security Plan**

4.1 The Service Provider shall ensure that a Security Plan which meets the requirements of this paragraph 4 (the "**Security Plan**") is:

(A) initially Approved in accordance with the Implementation Plan; and

(B) subsequently refined, expanded and amended by the Service Provider and Approved by TfL:

(1) in accordance with the Implementation Plan (and, in any event, prior to the Operational Commencement Date);

(2) after any amendment to the Security Policy;

(3) within ten (10) Business Days, or such other period as may be expressly agreed in writing by the Parties following the implementation of a Change so as to incorporate the effects of that Change into the Security Plan; and

(4) formally reviewed every twelve (12) months from the Operational Commencement Date.

and in each case, the Service Provider shall submit a copy of the Security Plan and the review provided pursuant to paragraph 4.1(B) (as applicable) to TfL for Approval.

4.2 The Security Plan shall set out the processes and procedures that the Service Provider will implement at the Service Provider's Premises and otherwise in relation to the System and the provision of the Services to ensure compliance with the Security Policy.

4.3 If and to the extent that any existing security policies and procedures in force at any of the Service Provider's Premises or that otherwise apply in relation to the System and the provision of the Services do not comply with the Security Policy, the Service Provider shall amend such security policies and procedures so as to conform with the Security Policy and set these out in the Security Plan (at no cost to TfL).

4.4 The Service Provider shall ensure that the Security Plan shall be consistent with this Schedule and with the Security Policy.

4.5 The Service Provider shall ensure that the Security Plan at all times includes:

(A) fully documented security processes as necessary and relevant for secure operation of the System and the provision of the Services (such process to be set out as an appendix in the Security Plan);

(B) fully documented security operating procedures as necessary and relevant for secure operation of the Services and the System (such process to be set out as an appendix in the Security Plan);

(C) all security measures to be implemented and maintained by the Service Provider (and its Sub-Contractors) in relation to all aspects of the System

and Services including the Code of Connection (CoCo) (and any similar requirements) of any relevant Vehicle Data Service;

(D) a demonstration to validate that the current requirements of the Data Protection Act 1998 as may be amended or replaced from time to time are being met;

(E) a mapping to the provisions in the TfL Information Security Controls Framework (ISCF), (Annex 1 to this Schedule);

(F) without limitation to any other provision of this Agreement, the date or periods for reviews of, and updates to, the Security Plan in accordance with paragraph 4.1(B);

(G) the parameters of reviews and updates referred to in paragraph 4.5(A)-(E) (inclusive) above by the Service Provider, including:

(1) all new or changed threats to the System and the provision of the Services and relevant countermeasures;

(2) emerging good industry practice in relation to physical and logical security;

(3) responses to any Security Incident that occurred in relation to the System and the provision of the Services; and

(4) identification and enhancement of any security measure in relation to the System and the provision of the Services which fail to meet good industry practice.

(H) an obligation on the Service Provider and its Sub-Contractors to use industry standard disk-wipe software and other mechanisms conformant to the HMG IS5 Enhanced standard to render unusable all media that are no longer operational. This includes optical disks, floppy disks, hard disk drives, solid state storage, paper and tapes;

(I) without limitation to any other provision of this Agreement, the date or periods for reviews of, and updates to, the Security Plan;

(J) an acknowledgment that it complies with all relevant policies set out at Schedule 34 (*TfL Policies*) in relation to the security of the System and provision of the Services; and

(K) a description of how the delivered solution meets the requirements of this Schedule and Schedule 2 (*Statement of Requirements*).

5. **Security Principles**

5.1 The Service Provider acknowledges and agrees that security and Data and information confidentiality in connection with the System and the provision of the Services are of key importance and fundamental to the evidential and financial security requirements necessary to administer and operate the System and the Services and to retain public confidence.

5.2 The Service Provider shall, and shall ensure that its Sub-Contractors shall, at all times ensure that the System and the provision of the Services:

(A) avoid the security threats to the System in accordance with Schedule 2 (*Statement of Requirements*); and

(B) fully comply with:

(1) the Data Protection Act 1998 as amended or replaced from time to time;

(2) the TfL Information Security Controls Framework in Annex 1 to this Schedule as amended or replaced from time to time;

(3) all relevant policies set out in Schedule 34 (*TfL Policies*) relating to Security of the System and Services each as amended or replaced from time to time; and

(C) comply with the relevant components of Information Technology Security Evaluation Criteria (ITSEC), as amended and updated by Common Criteria for Information Technology Security Evaluation or ISO/IEC 15408 standards.

5.3 The Service Provider shall keep all Data, information, Service Provider's Premises, and the System secure and protected against all loss, damage, corruption, unavailability and unauthorised use, access or disclosure in accordance with standards not to fall below those standards:

(A) set out in this Schedule;

(B) set out in the Security Policy and the Security Plan;

(C) set out in Clauses 26 (*Loss of Software and Data Security*) and 37 (*Data Protection*);

(D) as set out in Schedule 2 (*Statement of Requirements*) and TfL's Information Security Classification Standard set forth in Schedule 34 (*TfL Policies*) as amended or replaced from time to time;

(E) consistent with good industry practice (for example, consistent with standards that are equal to or higher than those set out in CESG Data Handling Final Report – June 2008); and

(F) Consistent with the CPNI SCADA Security Guidance.

The Service Provider shall immediately notify TfL of any actual or threatened breach in connection with the security of the System or the provision of the Services.

5.4 The Service Provider shall ensure that Hardware used in the provision of any of the Services is not reused or is only reused in accordance with the Security Plan.

5.5 The Service Provider shall design and build, and apply any changes to, the System in such a way that the impact of exposure of Personal Data, Data relating to the System or the provision of the Services or its configuration that could pose a security risk and Data supplied by government agencies, to unauthorised parties is minimised (to the extent reasonably possible) including by ensuring partitioning/segmentation of Data occurs to the extent necessary to prevent retrieval of large volumes of aggregated Data in order to reduce the Data handling requirements that would be imposed by any government agency.

5.6 The Service Provider shall ensure that appropriate background security checks of all

Service Provider Personnel are performed before such Service Provider Personnel are permitted to access the Services or the System.

5.7 The Service Provider's obligations in respect of physical security of Assets are set out in Schedule 2 (*Statement of Requirements*).

5.8 The Service Provider shall ensure that TfL Confidential Information and Personal Data transmitted over public networks is encrypted and transmitted securely in accordance with TfL's Information Classification Standard set forth in Schedule 34 (*TfL Policies*).

5.9 The Service Provider shall ensure that all transfers of Data between the Service Provider and external Third Parties are secure and transmitted in accordance with TfL's Information Classification Standard set forth in Schedule 34 (*TfL Policies*).

5.10 The Service Provider shall ensure that the System and the Services comply with Schedule 34 (*TfL Policies*), and the TfL Code of Connection Policy. Where appropriate, schemes requiring access to data from central or local UK Government must also comply with the government Code of Connection relating to the Public Sector Network (PSN).

(A) The Service Provider shall provide documentation stating explicitly how the scheme complies with the Code of Connection.

(B) The Service Provider shall provide documentation supporting compliance to TfL on an annual basis or as requested by TfL.

6. Security Classification

6.1 The Service Provider shall following the Operational Commencement Date, employ a CLAS consultant to determine the security classification appropriate to the Service Provider's proposed design.

6.2 The Service Provider shall design and implement the controls, processes and procedures required to comply with such security classification.

6.3 TfL may from time to time specify changes to the appropriate security classification at which the Service Provider shall protect and keep secure all data, information, Service Provider's Premises and System and the Service Provider shall design and implement the controls, processes and procedures required to comply with such security classification. To the extent that the security classification specified by TfL requires any changes to the Requirements, the impact of such changes shall be considered and implemented in accordance with Schedule 9 (*Change Control Request Procedure*).

7. Notification and Reporting of Security Incidents

7.1 The Service Provider shall, and shall ensure that its Sub-Contractors shall:

(A) promptly identify all Security Incidents;

(B) immediately:

(1) classify each Security Incident according to the Severity Levels (if appropriate) as defined in this Agreement); and

(2) record each Security Incident and corresponding Severity Level in the Incident log;

(C) where a Security Incident involves Personal Data, notify TfL as soon as possible and in any event in accordance with the timeframes of the corresponding Severity Level as defined in this Agreement; and

(D) provide monthly Security Incident reports detailing any Security Incidents to TfL in accordance with the Incident management process and Schedule 10 (*Contract Management and Reporting*).

7.2 Without limitation to the other provisions of this Agreement, the Service Provider agrees that each Security Incident will be classified as Severity 1 or Severity 2 (as TfL may instruct), unless the Service Provider can demonstrate to TfL's satisfaction that a classification of Severity 3 or lower would be more appropriate.

7.3 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.

8. **Security Incident and Event Management (SIEM) Solution**

8.1 The Service Provider shall develop and comply with a SIEM solution and shall submit such a solution to TfL for Approval, prior to the Operational Commencement Date and maintain the SIEM solution throughout the Term.

8.2 The Service Provider shall ensure that the SIEM solution aggregates data from the System(s) sources, including without limitation the

(A) network;

(B) firewalls;

(C) servers;

(D) Interfaces;

(E) databases; and

(F) applications.

8.3 The Service Provider shall ensure that the SIEM solution correlates data attributes and links Security Incidents and 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.

8.4 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 Service Provider's Personnel and TfL Personnel immediately.

8.5 The Service Provider shall ensure that the SIEM solution analyses security event information to assist the Service Provider in pattern identification and to highlight any activities that do not conform to a standard pattern.

8.6 The Service Provider shall ensure that the SIEM solution automatically gathers information about security event information and generates reports suitable for security, governance and auditing processes.

8.7 The Service Provider shall ensure that the SIEM solution stores historical Data to facilitate correlation of Data over time and to provide the retention necessary to satisfy compliance requirements in accordance with Schedule 2 Appendix 12 (*Data Retention*).

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

8.9 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 Approval.

8.10 The Service provider shall ensure that all aggregated and historical SIEM Data is secured with 'read only' access.

8.11 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 Approval in accordance with Schedule 3 (*Milestones and Deliverables*).

8.12 The Service Provider shall ensure that the SIEM solution mitigates the effect of any potential and/or actual breach of security.

8.13 The Service Provider shall provide all mitigations to TfL for Approval.

8.14 The Service Provider shall ensure that no Authorised 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:

(A) Data Base Administration (DBA);

(B) Authorised User account maintenance;

(C) maintenance of system files such as System logs, backup files and various data extracts provided to TfL;

(D) network maintenance including any security and communications software; and

(E) Hardware maintenance.

8.15 The Service Provider shall ensure the System retains SIEM logs in accordance with Schedule 2 Appendix 12 (*Data Retention*).

8.16 If a Security Incident occurs:

(A) the Service Provider shall as soon as possible (at no cost to TfL) correct, make good, reinstate, replace and fix all deficiencies, loss and/or damage to the System and/or provision of the Services in connection with a Security Incident, and/or perform or re-perform Tests or alternative Tests relating to the security of the System and/or provision of the Services, as appropriate, including within timeframes specified by TfL from time to time, to demonstrate to TfL's satisfaction that the relevant parts of the System and/or Services provide the features, functions, and facilities and meet the performance criteria specified in the Requirements and this Agreement including in connection with the Service Provider implementing any Security Rectification Plan pursuant to section 8.16(B);

(B) the Service Provider shall immediately and at the Service Provider's cost prepare a Security Rectification Plan including full details of the steps to be taken by the Service Provider to perform its obligations under section 8.16(A) and shall, without limiting section 8.16(A), submit a copy of that Security Rectification Plan to the TfL for its Approval and, subject to such Approval, the Service Provider shall fully implement and comply with that Security Rectification Plan (the "**Security Rectification Plan**");

(C) the Service Provider shall promptly escalate the matter to such level of seniority within the Service Provider's Personnel as TfL may require; and/or

(D) TfL may exercise its rights under Clauses 43 (*Enhanced Co-operations and Remedy Plans*) and 29 (*Step In Rights*).

8.17 The Service Provider shall provide a detailed report to TfL within forty eight (48) hours of the resolution of a Security Incident. This report shall detail:

(A) the nature of the Security Incident;

(B) the causes and consequences of the Security Incident;

(C) the actions taken to handle the Incident and timeframes applicable to resolution of the Security Incident; and

(D) actions to prevent recurrence of the Security Incident.

9. Testing of the Security Plan

The Service Provider shall, in relation to the Security Plan and at no additional cost to TfL conduct Tests to assure compliance with the Security Plan and with the Security Policy, the security provisions in this Agreement and this Schedule. Testing should be conducted in accordance with Schedule 4 (*Testing Regime*) and make the results available to TfL upon request. Such security Tests must be conducted prior to the Operational Commencement Date, and as a minimum, every twelve (12) months from the Operational Commencement Date.

10. Auditing

10.1 The Service Provider shall at least once within each twelve (12) month period from the Operational Commencement Date, engage an appropriately skilled Third Party to conduct a formal Data Protection Audit of the System and the provision of the Services against the then current versions of the following:

(A) the Security Plan; and

(B) the controls, processes and procedures put in place or required pursuant to this Agreement.

10.2 The Service Provider shall at least once within each twelve (12) month period from the Operational Commencement Date, engage with TfL and agree the scope and method of audit for ensuring that the Hardware and Services are compliant with the TfL Information Security Controls Framework as specified in Annex 1 to this Schedule.

10.3 Within ten (10) Business Days, or such other period as may be agreed in writing by

the Parties, the Service Provider shall develop a Remedy Plan to address the recommendations of any audits carried out, in accordance with paragraph 10.1.

10.4 This Remedy Plan shall include dates by which the recommendations will be required to be implemented by the Service Provider.

10.5 The Service Provider shall ensure that the Remedy Plan is implemented promptly and at no cost to TfL.

10.6 The Service Provider shall ensure that TfL and TfL Representatives are granted access to the System and Premises as and when requested for the purposes of auditing.

10.7 The Service Provider shall, and shall procure that its Sub-Contractors shall, contain equivalent rights of audit, inspection and access in favour of TfL (and any Third Party to whom rights of audit, inspection and access are granted).

10.8 The Service Provider shall, at no additional cost to TfL, provide full co-operation for any audit including but not limited to access to the System, Documentation and Personnel used to deliver the Services.

11. **Records for Auditing**

11.1 The Service Provider shall, and shall ensure that its Sub-Contractors shall, maintain a complete, current and accurate set of Records pertaining to all activities relating to the provision of the Services for the purposes of audits.

11.2 The Service Provider shall, and shall ensure that its Sub-Contractors shall retain all such Records for a period of not less than six (6) years (or such longer period as may be prescribed by Law) following termination or expiry of the Agreement and at the end of such period TfL may require that a subset of documents relevant to its then existing requirements be delivered by the Service Provider to TfL.

11.3 The Service Provider shall ensure that the Records include, but not be limited to:

(A) records of all Service Provider Personnel involved in the provision of the Services including names, training records, timesheets and National Insurance numbers;

(B) Sub-Contracts (including proposals of successful and unsuccessful bidders, bids and rebids), commitments, leases, manufacturer's specifications and details, purchase orders and data relating to procurement of the Services or any part of the Services;

(C) management accounts, information from Management Information Systems and any other management records;

(D) accounting records;

(E) original estimates;

(F) estimating worksheets;

(G) correspondence;

(H) variation, claims and compensation events files (including documentation covering negotiated settlements);

(I) detailed inspection records;

(J) information relating to each and all System Failures; and

(K) any other information specified in this Agreement.

12. **Threat Risk and Vulnerability Approach**

12.1 The Service Provider shall agree with TfL an approach for the review and mitigation of risks.

12.2 The Service Provider shall ensure that risks, vulnerabilities and threats shall be formally documented and reviewed at least quarterly with TfL.

13. **Anti-Malware Scanning and Protection**

13.1 The Service Provider shall provide all Service Provider Personnel with induction and ongoing training in the processes and procedures used to protect the System from Viruses, and in how to manage the impact of such attacks in accordance with the Incident management process.

13.2 The Service Provider shall ensure that all procedure manuals related to anti-malware protection are readily available to all relevant Service Provider's Personnel.

13.3 All computer Hardware used in connection with providing the Services shall be dedicated as such and be regularly scanned for Viruses.

13.4 All Hardware delivered to TfL, or used in connection with providing the Services or used by the Service Provider in providing the Services, shall be locked down to prevent any Authorised Users having access to:

(A) USB;

(B) CD/DVD drives; and

(C) other external media devices.

This shall include any computer devices used by the Service Provider to provide System support, whether the device is used remotely, or is located in a site used by the Service Provider. The Service Provider shall ensure that only System Administrators shall have access to these devices.

13.5 The Service Provider shall ensure that all new Hardware being introduced into the System, whether for support or as part of the System, shall be Tested, verified and certified as being free from any Viruses before being connected.

13.6 The Service Provider shall pro-actively maintain protection against Viruses, Spyware, Malware and other potentially destructive software, including the continued identification and protection against new threats, at no additional cost to TfL.

13.7 The Service Provider shall manage the impact of attacks by Viruses, spyware, malware and other potentially destructive software in accordance with the Approved Incident management process.

13.8 The Service Provider shall develop and comply with a policy for maintaining the latest versions of leading industry protection software to address risks of Virus and unauthorised access to the System and shall submit such a policy to TfL for

Approval, the ("**Security Patch Processing Policy**").

13.9 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 System and related software.

14. Security and Audit Logs

14.1 The Service Provider shall maintain a log of all accounts used by all Authorised Users. This log shall include: all creations, all deletions, all IT system group memberships, all Authorised User and group privilege changes against each of the System resources.

14.2 The Service Provider shall implement a process which will verify and validate all files transferred onto and from the System. This process will include controls which ensure that only authorised files are transferred by using principles of segregation of duties (so that no person is given responsibility for more than one related function, for example, a person creating content to be uploaded into the System must not be able to load such content themselves and a different person will be responsible for the verification, validation and upload functions).

14.3 The Service Provider shall implement a mechanism to strictly control and limit the application programs that can be executed. Only programs necessary for the correct operation of the System shall be permitted to execute. The Service Provider shall formally record these permitted programs, along with version numbers and justifications for executing any such programs and must log all attempted violations, such log to record (without limitation);

(A) the name of the Authorised User attempting to execute an unauthorised program;

(B) the date and time of the attempt; and

(C) the IP address of the system.

Any such violation attempt must be recorded as a Security Incident and investigated to identify the root cause.

14.4 The Service Provider shall provide system audit log data (being any log data that is collected by the Service Provider during the delivery of the Services) to TfL on request, in a human readable electronic format. Acceptable formats are Comma Separated Value or Microsoft Excel.

14.5 The Service Provider shall ensure that appropriate resources are available and that auditable electronic records of scheduling and cancellations are kept for the purposes of audits.

14.6 The Service Provider shall ensure that all Records are in a human readable format.

15. Security Management

15.1 The Service Provider shall propose a member of the Service Provider's Personnel as Security Manager to TfL for Approval and, when Approved, shall appoint such person.

15.2 The Service Provider shall ensure that the Security Manager shall provide a security management service to develop, monitor, enforce, maintain and enhance all aspects

of the Security Plan throughout the Term.

15.3 The Service Provider shall ensure that the security management service, as defined in 15.2 above, includes, but is not limited to, the publication and communication to TfL within ten (10) Business Days, or such other period as may be expressly agreed in writing by the Parties of the preceding month a monthly Security Incident report that gives an overview of the security performance of the System and the provision of the Services for that month. The format of this report will be reviewed prior to the Operational Commencement Date with TfL, but initially it will include details such as:

(A) the incident number of each Security Incident during the month, including a nil return if applicable;

(B) an overview of any Changes, which impact security of the System or the provision of the Services, that have been implemented in the month;

(C) an overview of any Changes, which impact security, planned to be implemented during the next month;

(D) details of the last audit, to include but not limited to the date of the last action;

(E) details of the next audit, to include but not limited to the date of the next action;

(F) details of any risk reviews, or new risks identified in last month; and

(G) details of any Incidents that have impacted on security, or had the potential to impact on security, identified in last month.

15.4 The Service Provider shall provide the monthly Security Incident report to TfL in accordance with the Incident management process and Schedule 10 (*Contract Management and Reporting*);

15.5 TfL will be responsible for issuing passes to its Premises on request. Some buildings are open 'office hours' only and some special areas are 24 (twenty-four) hours to pass holders. For general access the holder will require a Disclosure and Barring Service (DBS) check, this will give access to all non-secure areas of TfL's Premises. Where staff require regular un-escorted access to the control room environment the Service Provider shall demonstrate to TfL's satisfaction that the Service Provider's Personnel have appropriate security clearance which is equivalent to the Non-Police Personal Vetting Level 2 clearance required.

16. **Authorised User Access Management**

16.1 The Service Provider shall implement a system to manage access rights to the System (the "**Access and Identity Management Solution**").

16.2 The Service Provider shall ensure that the Access and Identity Management Solution shall:

(A) support different roles within the System;

(B) enforce the level of access which those roles can achieve;

(C) ensure roles can only be changed by System Administrators; and

(D) log all change activities (this includes changing Authorised User roles and role functions).

16.3 The Service Provider shall ensure that the Access and Identity Management Solution shall differentiate between application logon roles and system level roles (i.e Enforcement Officer and System Administrators).

16.4 The Service Provider shall ensure that the Access and Identity Management Solution shall ensure for certain roles all Operating System level access roles (i.e. System Administrators) remote access will be restricted to fixed devices on fixed IP addresses and shall use a secure virtual private network with complex authentication. The Service Provider shall work with the Third Party who will be providing telecommunications Services in connection with the System or the Services to achieve the optimum solution.

16.5 The Service Provider will provide details to TfL of all other roles requiring remote access. The appropriate security controls applicable to such access can be discussed and agreed between the Parties before such access is granted and once Agreed, TfL will authorise the request.

16.6 The Service Provider shall manage and ensure that Personnel who will maintain Hardware within TfL's Premises or other buildings have the Counter Terrorism Check (CTC) security clearance.

16.7 The Service Provider shall notify TfL on any changes that affect an individual workers security clearance.

16.8 The Service Provider shall ensure that TfL Personnel are allocated access permissions to the System as required by TfL.

16.9 The Service Provider shall ensure that the Access and Identity Management Solution verifies that the requestor has a legitimate reason for accessing the System.

16.10 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 Authorised User (for example, the Service Provider shall ensure that a person cannot submit and authorise their own access).

16.11 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.

16.12 The Service Provider shall ensure that the identity of each Authorised User is authenticated before using any System.

16.13 The Service Provider shall ensure that the identity of the Service Provider's Personnel or Authorised Users and their location is authenticated before using the System.

16.14 The Service Provider shall ensure that TfL Personnel are allocated access permissions to the System as and when requested in writing by TfL

16.15 The Service Provider shall ensure that TfL Authorised Users have access to the System from TfL Approved locations.

16.16 The Service Provider shall ensure that the Access and Identity Management Solution logs the credentials of all Authorised Users accessing the System for the purposes of audits.

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

16.18 The Service Provider shall ensure that where an Authorised User accesses the System remotely for the purposes of Service Management, that Authorised User shall not have access to Personal Data.

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

16.20 The Service Provider shall ensure that credentials used to authenticate Authorised Users are held securely within the System and that the System prevents unauthorised access and retrieval of such credentials.

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

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

16.23 The Service Provider shall develop and comply with policies for maintaining the security of all passwords and shall submit such policies to TfL for Approval prior to the Operational Commencement Date in accordance with Schedule 3 (*Milestones and Deliverables*) and shall enforce these Approved policies for the Term.

16.24 The Service Provider shall ensure that the policies for maintaining the security of all passwords shall be in accordance with Annex 1 (*Information Security Controls Framework (ISCF)*) to this Schedule and may be amended, and/or superseded from time to time.

16.25 The Service Provider shall not grant access to the System for any Third Party without the prior written Approval of TfL.

16.26 The Service Provider shall immediately, upon notification from TfL, disable an Authorised User's logon and access rights when the Authorised User is a member of TfL Personnel and ceases to be a member of TfL Personnel.

16.27 The Service Provider shall ensure that when a member of the Service Provider's Personnel is dismissed or leaves, all property belonging to the Service Provider are returned; accesses are revoked and the individual is escorted from the Premises on their last day.

17. **Penetration and Vulnerability Tests**

17.1 The Service Provider shall at least once within each twelve (12) month period from the Operational Commencement Date, engage an appropriately skilled Third Party to undertake a Penetration Test and Vulnerability Assessment.

17.2 Penetration and Vulnerability tests undertaken will be at no cost to TfL.

17.3 The Service Provider shall provide a copy of the final assessment report to TfL

17.4 Within ten (10) Business Days, or such other period as may be agreed in writing by the Parties, the Service Provider shall, at its own cost, remedy any deficiencies to the System where such deficiencies breach this Agreement.

18. Combined Workstation Requirements

18.1 The Service Provider shall ensure that access to Combined Workstations is subject to appropriate authorisation for access controls in accordance with the TfL Information Security Controls Framework (Annex 1 to this Schedule 14) and may be amended, and/or superseded from time to time.

18.2 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.

18.3 The Service Provider shall grant each Authorised User the minimum access permissions required for that Authorised 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.

18.4 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 any Hardware in connection with this Agreement.

18.5 The Service Provider shall immediately disable an Authorised User's logon and access rights when an Authorised User ceases to be a member of the Service Provider's Personnel, or an Authorised User ceases to work on delivering or operating any Hardware in connection with this Agreement.

19. Removable Media

19.1 The Supplier may only use removable media to support its delivery of the Services if it has obtained prior written consent of TfL and has implemented appropriate controls to ensure that the use of any input or output devices and removable media is restricted strictly to that needed to supply and support delivery of the Services.

19.2 The Supplier shall ensure that all Supplier Personnel with access to removable media are subject to acceptable use policies, on-going risk management procedures and appropriate training. Such policies and procedures shall be designed to discourage the use of removable media and protect the integrity of removable media.

19.3 If removable media is approved for use by TfL, the Supplier shall ensure that it deploys suitable anti-virus and anti-malware checking solutions to actively scan for the introduction of malware onto systems and networks through all Data imports and exports from removable media and that the removable media is encrypted to a suitable standard agreed in advance with TfL in writing.

19.4 The Supplier shall report any loss or interception of Data or TfL Data as a result of the use of removable media to TfL in accordance with Paragraph **Error! Reference source not found.** and TfL reserves the right in such instances to rescind its approval in relation to the Supplier's continued use of removable media.

20. Mobile and Home Working

20.1 If the Supplier does not have a home and mobile working policy for Supplier Personnel, TfL's home and mobile working policy shall apply to the Supplier and its

Supplier Personnel.

20.2 If the Supplier has a home and mobile working policy in relation to the Supplier Personnel, the Supplier shall:

(a) ensure through this policy that:

(i) Data and TfL Data is protected and suitably encrypted when stored outside of the Supplier Premises;

(ii) Data and TfL Data is protected when accessed, imported or exported through a connection other than one which is accessed at the Supplier Premises; and

(iii) Security Incident management plans acknowledge the increased risk posed by home and mobile working such as theft or loss of Data and TfL Data and/or devices; and

(b) submit such policy to TfL for Assurance.

(c) The Supplier shall report any loss or interception of Data or TfL Data as a result of home or mobile working to TfL in accordance with Paragraph **Error! Reference source not found.**.

ANNEX 1

Information Security Controls Framework (ISCF)

Please refer to the accompanying PDF document entitled Information Security Controls Framework.pdf.

ANNEX 2

Security Policy

ANNEX 3

Security Plan