SCHEDULE 2.4

SECURITY MANAGEMENT

LOT 2

VERSION CONTROL

VERSION NUMBER	DATE	COMMENT
1.0	July 2021	Execution Version

CONTENTS

1	PURPOSE	1
2	SECURITY POLICY	1
3	SECURITY MANAGEMENT PLAN	2
4	THE SUPPLIER	3
5	NOTIFICATION AND REPORTING OF SECURITY INCIDENTS	3
6	TESTING OF THE SECURITY MANAGEMENT PLAN	4
7	AUDITING	4
8	TFL SPECIFIC REQUIREMENTS	4

SCHEDULE 2.4 – SECURITY MANAGEMENT

1. PURPOSE

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

1.1.1 TfL's security requirements relating to the Supplier Assets and the provision of Services; and

1.1.2 the development, updating and testing of the Security Policy and Security Management Plan.

2. SECURITY POLICY

2.1 The Supplier shall ensure that a Security Policy which meets the requirements of this paragraph 2 is initially approved in accordance with the Transition Plan and the Supplier shall subsequently, at its own cost;

2.1.1 refine, expand and amend the Security Policy:

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

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

2.1.2 promtly prepare a written review of the Security Policy (as the same may be amended from time to time in accordance with paragraph 2.1.1(b) upon request from TfL from time to time and in any event at least once in every twelve (12) month period following the Operational Commencement Date,

and in each case, the Supplier shall submit a copy of the Security Policy and the review provided pursuant to paragraph 2.1.2 (as applicable) to TfL for approval in accordance with the process detailed in Schedule 8.6 (Document Management).

2.2 The Supplier shall ensure that the Security Policy shall:

2.2.1 include specific detail related to the Services and the Supplier Assets;

2.2.2 reference and comply with, and be consistent with, this Schedule;

2.2.3 reference and comply with the security requirements set out in Schedule 2.1 (Statement of Requirements);

2.2.4 comply with

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

(b) TfL's security requirements in respect of the Supplier Sites in accordance with this Schedule;

(c) the TfL Information Security Classification Standard set out in Schedule 2.3 (Standards); and

(d) the TfL Information Security Controls Framework set out in Schedule 2.3 (Standards)

2.2.5 comply with such other requirements that TfL may reasonably request from time to time.

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

3. SECURITY MANAGEMENT PLAN

3.1 The Supplier shall ensure that a Security Management Plan which meets the requirements of this paragraph 3 is:

3.1.1 initially approved in accordance with Transition Milestone MS1; and

3.1.2 subsequently refined, expanded and amended by the Supplier and approved by TfL via the process detailed in Schedule 8.6 (Document Management);

(a) in accordance with the Transition Plan;

(b) after any amendment to the Security Policy;

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

(d) once every twelve (12) months from the Operational Commencement Date.

3.2 The Security Management Plan shall set out the processes and any security operating procedures that the Supplier will implement at the Supplier Sites and otherwise in relation to the Supplier Assets and the provision of the Services to ensure compliance with the Security Policy.

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

3.4 The Supplier shall ensure that the Security Management Plan shall be consistent with this Schedule and with the Security Policy.

3.5 The Supplier shall ensure that the Security Management Plan at all times includes:

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

3.5.2 without limitation to any other provision of this Agreement, the date or periods for reviews of, and updates to, the Security Management Plan in accordance with paragraph 3.1.2;

3.5.3 the parameters of reviews and updates referred to in paragraphs 3.5.1 and 3.5.2 (inclusive) above by the Supplier, including:

(a) new or changed threats to the Supplier Assets and the provision of the Services and relevant countermeasures;

(b) emerging Good Industry Practice in relation to physical and logical security

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

(d) identification and enhancement of any security measure in relation to the Supplier Assets and the provision of the Services which fail to meet Good Industry Practice.

4. THE SUPPLIER

4.1 The Supplier acknowledges and agrees that security and data and information confidentiality in connection with the Supplier Assets and the provision of the Services are of key importance to conduct the Services and to retain public confidence

4.2 The Supplier shall, and shall procure that its Sub-Contractors shall, at all times ensure that the Equipment and the provision of the Services:

4.2.1 are protected from security threats in accordance with the approved Security Policy and Security Management Plan for all Sites and Equipment; and

4.2.2 act in accordance with:

(a) the Data Protection Laws;

(b) the TfL Information Security Controls Framework as referred to in Schedule 2.3 Standards;

(c) the TfL Information Security Classification Standard as referred to in Schedule 2.3 (Standards); and

as amended or replaced from time to time;

4.3 The Supplier shall keep all data, licence documentation, information, Supplier Sites, Vehicle Inspection Sites and the Supplier Assets 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

4.3.1 set out in this Schedule;

4.3.2 set out in the Security Policy and the Security Management Plan;

4.3.3 as set out in Schedule 2.1 (Statement of Requirements) and TfL's Information Security Classification Standard as referred to in Schedule 2.3 (Standards);

4.3.4 consistent with Good Industry Practice.

4.4 The Supplier shall immediately notify TfL of any actual or threatened breach in connection with the security of the Supplier Assets or the provision of the Services.

5. NOTIFICATION AND REPORTING OF SECURITY INCIDENTS

5.1 The Supplier shall, and shall procure that its Sub-Contractors shall alert TfL immediately upon discovery of any suspected breach of security of a Supplier Site.

5.2 If a Security Incident occurs which is Service affecting:

5.2.1 the Supplier shall as soon as possible correct, make good, reinstate, replace and fix all Faults, loss and/or damage to the Supplier Assets and/or provision of the Services.

5.2.2 the Supplier shall promptly escalate the matter to the Commercial Manager

6. TESTING OF THE SECURITY MANAGEMENT PLAN

6.1 The Supplier shall, in relation to the Security Management Plan and at no additional cost to TfL conduct tests to assure compliance with the Security Management Plan and with the Security Policy, the security provisions in this Agreement and this Schedule. Such security tests must be conducted, as a minimum, every twelve (12) months from the Operational Commencement Date and the results shall be made available to TfL.

7. AUDITING

7.1 The Supplier shall conduct annual security audits to ensure security processes and procedures are adhered to and the results shall be made available to TfL.

8. TfL SPECIFIC REQUIREMENTS

8.1 In addition to its other obligations in this Schedule, the Supplier shall comply with the following specific requirements:

8.1.1 Anti-Malware Scanning and Protection

(a) the Supplier shall provide all members of the Supplier's Personnel with induction and ongoing training in the processes and procedures used to protect from viruses, and in how to manage the impact of such attacks.

(b) the Supplier shall ensure that all procedure manuals related to anti-virus protection are readily available to all relevant members of the Supplier's Personnel

(c) all computer hardware used in connection with providing the Services shall be dedicated as such and be regularly scanned for viruses.

(d) all computer hardware delivered to TfL, or used in connection with providing the Services or used by the Supplier in providing the Services, shall be locked down to prevent any users having access to:

(i) USB devices and ports

(ii) CD/ DVD drives; and

(iii) Other external media devices

(e) this shall include any computer devices used by the Supplier to provide Services support, whether the device is used remotely, or is located at the Supplier's Site. The Supplier shall ensure that only the Supplier's Personnel providing Services as part of this Agreement shall have access to these devices.

(f) the Supplier shall ensure that all new hardware being introduced into the Supplier Assets, shall be tested, verified and certified as being free from any viruses before being connected

8.2 Security Management

8.2.1 the Supplier shall appoint a member of the Suppliers Personnel as Security Manager.

8.2.2 the Supplier shall ensure that the Security Manager shall provide a security management service to develop, monitor, enforce, maintain and enhance all aspects of the Security Management Plan throughout the Term.

8.2.3 the Security Manager shall provide a report providing an overview of security-related activities for each Period. This shall be included as part of the Service Delivery Group. This overview shall include the following;

(a) an overview of any changes, which impact security of the Supplier Assets or the provision of the Services, that have been implemented in the relevant Period;

(b) an overview of any changes, which impact security, planned to be implemented during the following Period;

(c) details of the last audit, to include but not be restricted to the date of the last action

(d) details of the next audit, to include but not be restricted to the date of the next action;

(e) details of any risk reviews, or new risks identified in the relevant Period; and

(f) details of any Security Incidents, or circumstances that had the potential to have an impact on security and/or become a Security Incident.

8.3 Key and Pass Management

8.3.1 the Supplier shall be responsible for the safe keeping of any keys and passes issued to the Supplier’s Personnel.

8.3.2 the Supplier shall promptly report any loss of keys and/or passes to the Commercial Manager.

8.3.3 the Supplier shall replace, at the Supplier's expense, any lost keys and/or passes, at the earliest opportunity.