Transport for London

SCOPE

APPENDIX V
Cyber Security

CYBER SECURITY MANAGEMENT SCHEDULE

TABLE OF CONTENTS

Contents

DEFINITIONS 3
1. PURPOSE 5
2. SECURITY PRINCIPLES 5
3. ACCESS CONTROLS AND SECURE CONFIGURATION OF SYSTEMS 6
4. *THE CONTRACTOR'S* PEOPLE 7
5. TRAINING 7
6. TESTING & AUDIT 8
7. SECURITY INCIDENT MANAGEMENT PROCESS 9
8. SECURITY LOGGING AND MONITORING 11
9. MALICIOUS SOFTWARE 12
10. REMOVABLE MEDIA 13
11. MOBILE AND HOME WORKING 13
12. DISPOSALS 14
13. SECURITY MANAGEMENT PLAN 14
14. INFORMATION SECURITY MANAGEMENT SYSTEM 15
15. COMPLIANCE WITH ISO/IEC 27001 16
16. APPROVED PRODUCTS 16

DEFINITIONS

"Cloud"	A type of internet-based computing service where organisation can have aspects of their IT infrastructure managed by external providers, normally as a Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) basis
"Cyber Essentials Scheme"	is a UK government scheme encouraging organisations to adopt good practice in information security, focussing mainly on technical controls rather than governance, risk, and policy
"Cyber Security Policy / Policies"	The high level Cyber Security requirements for all IT and Operational technology and data owned by TfL or operated and supported by third parties for on behalf of TfL.
"Cyber Security Standard(s)"	The technical detail behind the implementation of the high level cyber security requirements as set out in the Cyber Security Policies.
"Data"	means data created, generated or collected, during Providing the Services (or any part thereof), including Personal Data and data supplied to TfL and members of the TfL Group.
"Good Industry Practice"	means the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced operator engaged in the same type of undertaking under the same or similar circumstances.
HMG Information Security Assurance Standards	the meaning and definition as well as relevant policy documents and standards can be found at https://www.gov.uk/government/collections/government-security or any updated link;
"Information Asset Register"	means a register of all information assets relating to the *services* as detailed in paragraph 3.2(c)
"Information Security Management System" or "ISMS"	a framework of governance models, policies and procedures, based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security in accordance with the requirements of Paragraph 15
ISO/IEC 27001	is an information security standard specification for an information security management system (ISMS), with an emphasis on measuring and evaluating how well an organisation's ISMS is performing.
"IT Services"	means the IT services that support the delivery of the Services;
"Malicious Software"	means any software that brings harm to a computer system. Commonly known as malware can be in the form of worms, viruses, trojans, spyware, and adware which steal protected data, delete documents or add software not approved by a user.
"Operational Technology"	means any hardware or software which monitors and/or operates a physical process.
"Outline	means the security plan provided by the *Contractor* as part of their

Security Management Plan"	tender submission
"Removable Media"	any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, as well as diskettes and USB drives
"Security Incident"	a potential or actual event or attempted breach of security affecting the confidentiality, integrity or availability of the Services, IT Services or Networks which process or hold Data
"Security Management Plan"	means the *Contractor*'s security plan developed and revised pursuant to Paragraph 14
"Security Policy"	means any TfL security policies as amended by TfL from time to time;
"Security Risk"	meaning all Risks associated with the security of the Services which may have a negative impact upon the agreed security posture, including information security and any risks identified pursuant to the Security Management Schedule.
"Security Risk Register"	means a register of Security Risks produced and maintained as detailed in paragraph 3.2(b)
"Service Assets"	means all information technology assets and rights including all physical assets, Software, IPR, as well as spares and components whether in storage, repair or on sites, used by the *Contractor* to Provide the Services.
"The *Contractor's* people"	means all employees, agents, consultants and contractors of the *Contractor* or of any Sub-Contractor
"*Contractor* Premises"	means any land or building where the *Contractor* carries out any part of this contract
"TfL Information Security Controls Framework"	means a hierarchy of IT security documents consisting of the high level Information Management Security Policy and ten security principles (Information Security Controls Framework).
"TfL Network(s)"	means the network infrastructure and services owned or used by TfL to support the delivery of the IT Services.
"TfL Personnel "	means all employees, agents, consultants and contractors of TfL
"TfL Restricted"	as defined in the TfL Information Security Classification Standard (listed in Annex 5)
"TfL Sites"	means all TfL premises where the services are delivered

1. PURPOSE

1.1 The purpose of this appendix to the Scope is to set out:

(a) the principles of protective security to be applied by the *Contractor* in iProviding the Service;

(b) the *Contractor*'s wider security obligations relating to Providing the Service;

(c) the *Contractor*'s requirements to test and audit Providing the Service including any Information Security Management Systemparagraph 3, to ensure compliance with the security requirements set out in this appendix to the Scope;

(d) the *Contractor*'s obligations in the event of a Security Incident;

(e) the principles for the *Contractor*'s development, implementation, operation, maintenance and continual improvement of the Security Management Plan;

(f) the principles for the *Contractor*'s development, implementation, operation, maintenance and continual improvement of the Information Security Management System;

(g) any obligations for certification against Providing the Service including but not limited to ISO/IEC 27001, the Cyber Essentials Scheme or HMG Information Security Assurance Standards;

(h) any requirements to Provide the Service in accordance with the CESG Commercial Product Assurance (CPA) Scheme

(i) the requirements on the *Contractor* when Providing the Service, which are aligned with the 10 Steps to Cyber security set out by the Government (see Annex 5) and

(j) the *Contractor's* obligation to comply with the Operations Technology Cyber Security Standards (see Annex 5).

2. SECURITY PRINCIPLES

2.1 The *Contractor* acknowledges that security, data protection and confidentiality are of fundamental importance in relation to its provision of the service and TfL's ability to retain public confidence. The *Contractor* shall at all times comply with the security principles set out in Paragraph 3 in Providing the Service.

2.2 In recognition of the importance that the *Client* places on security, data protection and confidentiality, the *Contractor* shall ensure that a director or relevant individual, as agreed by the *Service Manager*, is made aware of the risks set out in the Security Management Plan and is assigned overall responsibility for ensuring that:

(a) appropriate members of the *Contractor* people take responsibility for managing the different levels of security risk and promote a risk management culture;

(b) a Security Risk Register is produced and maintained and that all Security Risks are documented in an appropriate manner and is included in any

contract risk register if one is in place. This Security Risk Register must be available for audit when reasonably required by TfL as set out in Clause 7 of this Schedule.

(c) an Information Asset Register is produced and maintained and that all information technology assets are documented in an appropriate manner in the Information Asset Register and shall identify the criticality of the relevant Service Assets in the delivery of the Services. This register must be available for audit when reasonably required by TfL as stated in Paragraph 7 of this Schedule and when a Security Incident occurs.

(d) supporting policies are implemented (where relevant) and communicated with the *Contractor's* people.

2.3 The *Contractor* shall, at all times ensure that:

(a) security threats to the service are minimised and mitigated;

(b) delivery of the service shall fully comply at all times with:

(i) any security requirements set out in Annex 3;

(ii) the agreed Outline Risk Management Processes and approach set out in Annex 2; and

(iii) Good Industry Practice.

2.4 The *Contractor* must notify TfL of any instances where software, applications, services or processes are hosted or run from the cloud that are not part of Providing the Service, and that host, process or connect with any of TfL Operational or IT technology, Data and Networks or handle TfL Data. The *Contractor* is responsible for ensuring that any such cloud services comply with this Cyber Security Management Schedule.

3. ACCESS CONTROLS AND SECURE CONFIGURATION OF SYSTEMS

3.1 The *Contractor* shall comply with all obligations relating to the patching and configuration management of Service Assets as set out in Annex 4 in addition to any specific obligations set out in Annex 4, the *Contractor* shall ensure that:

(a) security patches are applied to Service Assets as soon as possible in line with vendor recommendations in accordance with overall risk management;

(b) account management and configuration control processes are implemented to ensure that access to Service Assets by the *Contractor's* people is limited to the extent required for them to fulfil their roles in supporting of Providing the Service.

(c) when the *Contractor's* people change roles or no longer support Providing the service, access rights are revoked or reviewed;

(d) any system administration functionality is strictly controlled and restricted to those people who need to have access to such functionality and that the ability of the *Contractor's* people to change the configuration of the Service Assets is appropriately limited and fully auditable;

(e) *The Contractor's* people are informed of what constitutes acceptable access of operational or IT technology, Data and Networks and the consequences of non-compliance;

(f) any preconfigured passwords delivered with any Service Assets are changed prior to their implementation for use in Providing the Service;

(g) the Service Assets have appropriate devices, tools or applications in place to filter traffic or separate connections, such as industry standard firewalls and malicious software protection, to all public or private networks which are not controlled by or on behalf of TfL;

(h) all wireless functionality is secure; and

(i) software upgrades and patching must be managed appropriately and access to any software shall be granted using the principle of least privilege.

4. *THE CONTRACTOR'S* PEOPLE

4.1 The *Contractor* shall, appoint a member of the *Contractor's* people to be the security manager who shall be responsible for the development, monitoring, enforcement, maintenance and enhancement of all security measures set out in this appendix to the Scope (the "**Security Manager**").

4.2 The *Contractor* shall ensure that all *of it's people* are security screened or vetted and shall provide TfL within five (5) working days of the *starting* date, and every twelve (12) months thereafter, written confirmation that this obligation has been complied with.

4.3 The *Contractor* shall immediately notify the *Service Manager* if it becomes aware of any security clearance issues in relation to the *it's* people and the *Contractor* shall undertake any action requested by the *Service Manager* in relation to mitigating the impact of any such security clearance issues.

5. TRAINING

5.1 The *Contractor* shall ensure that all of the *Contractor's* people have undergone suitable security awareness training prior to their deployment and such security awareness training shall cover, as a minimum; account usage, malicious software, home and mobile working, use of removable media, audit and inspection and Security Incident reporting and data handling. The *Contractor* shall implement an up-to-date on-going programme of security awareness training for the *Contractor's* people throughout the *service period*.

5.2 The *Contractor* shall provide additional training to its people, which may be required following a Security Incident, the application of a patch or update, or any relevant change to the Scope.

5.3 The *Contractor* shall ensure that all of it's people are familiar with their responsibilities under applicable law and policies including, as a minimum, the Data Protection Legislation, the Security Policies set out in Paragraph 1 of this appendix to the Scope and policies in relation to the handling of protectively marked materials both during their employment and following the termination of or change to the terms of their employment.

6. TESTING & AUDIT

6.1 The *Contractor* shall conduct regular automated vulnerability scans the Service Assets, as agreed in the Risk Management Process and ensure that any identified vulnerabilities are appropriately mitigated or patched in line with the TfL Security Patching Standard (Annex 5), taking into consideration the risk posed to the Client and Providing the Service.

6.2 The Contractor shall conduct security tests, including ethical hacking and penetration tests, to assure compliance with the Security Incident Management Process, the security provisions in this appendix to the Scope, the Security Management Plan. The Contractor shall conduct security testing in accordance with the Security Management Plan. The Contractor shall conduct such security tests, as a minimum, every twelve (12) months from the starting date and shall include security penetration testing of the Service Assets and the associated technical infrastructure. Wherever the Service Assets are accessible from the internet or other such public network, the Contractor shall carry out security penetration tests from the internet or the public network.

6.3 The Contractor shall, within one (1) week of completion of the security provide a report to the *Service Manager* setting out the outcome of such security tests including all identified vulnerabilities and it's plans to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this appendix to the Scope.

6.4 The *Contractor* shall implement its plans to each identified vulnerability in accordance with the report delivered pursuant to Paragraph 7.2 save to the extent directed by the *Service Manager* in writing.

6.5 The *Contractor* shall, upon request by TfL, following a Security Incident, carry out such additional security testing over and above the obligations set out in Paragraph 7.2.

6.6 The *Client* shall be entitled to send a representative to witness the conduct of any audit or security tests carried out by or on behalf of the *Contractor*. The *Contractor* shall provide the *Service Manager* with the results of such audits (in a form agreed in advance) as soon as practicable after the completion of each audit or test.

6.7 In addition to complying with this document, PCI DSS where applicable and other relevant industry standards and Good Industry Practice, the *Contractor* shall at least once during each twelve (12) month period starting from the Service Commencement Date, engage an appropriately skilled third party to conduct a formal audit of the Service Assets against the then current versions of the:

(a) security controls, processes and procedures required pursuant to this appendix to the Scope;

(b) Data Protection Legislation (using BS10012 or another standard as agreed with TfL), where applicable; and

(c) Security Management Plan.

The *Contractor* shall inform the *Service Manager* of actual or potential security issues which impact or could impact Providing the Service within five (5) days of becoming

aware of them and shall keep the *Service Manager* up to date as the it investigates the nature and impact of such issue. Within five (5) days of the finalisation of audit findings, the *Contractor* shall provide the Service Manager a copy of all such findings which are relevant.

6.8 Without prejudice to any other right of audit or access granted to the Client pursuant to this appendix to the Scope or at law, the *Service Manager* or other representatives of the *Client* may carry out such audits in relation to security matters as are reasonably required to assess the *Contractor*'s compliance with the Information Security Management System and the Security Management Plan.

6.9 If any test or audit carried out reveals any non-compliance with this appendix to the Scope or vulnerability (and, in the case of a TfL audit, TfL has informed the *Contractor* thereof), the *Contractor* shall, as soon as reasonably practicable, provide TfL with a written plan to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this appendix to the Scope. The *Contractor* shall implement its plans to remedy each identified vulnerability in accordance with such report save to the extent directed by the *Service Manager*.

7. SECURITY INCIDENT MANAGEMENT PROCESS

7.1 The *Contractor* shall:

(a) establish, document and provide to the *Service Manager* a process to identify and respond to Security Incidents and mitigate the impact of such Security Incidents on Providing the Service, including assigning clearly defined roles and responsibilities to specific *Contractor* people;

(b) record each Security Incident and corresponding severity level in the *Contractor*'s ISMS; and

(c) without limitation to the other provisions of this appendix to the Scope, follow TfL's reasonable instructions in relation to the identification and resolution of any Security Incident.

7.2 The *Contractor* shall notify and ensure that the *Service Manager* is aware as soon as possible and in any event no later than within one (1) hour, upon becoming aware of any Security Incident or of any potential Security Incident.

7.3 The *Contractor* will additionally provide notification with all relevant details reasonably available of any actual or suspected breach of security in relation to any *Client* personal data including unauthorised or unlawful access or processing of, or accidental loss, destruction or damage.

7.4 If a Security Incident occurs, the *Contractor* shall:

(a) immediately take steps to assess the extent of the Data compromised or affected including, but not limited to, the amount of affected;

(b) immediately take the steps necessary to remedy or protect the integrity of the Service Assets against any such Security Incident;

(c) securely collect and preserve evidence, including logs, to support the Security Incident Management Process and share with the *Service Manager* such evidence;

(d) handle any information pertaining to the Security Incident according to the handling requirements for TfL RESTRICTED information defined in TfL's Information Security Classification Standard;

(e) promptly escalate the Security Incident to the Service Manager;

(f) when requested by TfL:

a. provide such information in relation to the Security Incident (including, if necessary, by collating such information from its and its Sub-contractors' systems and the *Contractor* Personnel);

b. provide the *Client's* representative with supervised access (or, if the Parties agree, direct access) to any relevant systems, *Contractor* Premises and peoplein order to investigate the Security Incident; and

c. follow the *Client's* directions in relation to the steps necessary or desirable to remedy or protect the integrity of the Service Assets; and

(g) as soon as reasonably practicable develop and provide TfL with a copy of its remediation plan for the Security Incident which sets out full details of the steps taken and to be taken by the *Contractor* to:

a. correct, make good, reinstate, replace and remediate all deficiencies and vulnerabilities, loss and/or damage to the Service Assets, Data, and/or Services in connection with the Security Incident; and

b. perform or re-perform any security tests or alternative tests relating to the security of the Service Assets and/or Services as appropriate and within the timescales specified by TfL, to assure TfL that the Security Incident has been addressed and its effects mitigated,

provided that any such remediation must be implemented in accordance with this appendix to the Scope. The *Contractor* shall fully implement and comply with any such remediation plan unless otherwise instructed by the Service Manager.

7.5 The *Contractor* shall provide a detailed report to TfL within two (2) days of the resolution of the Security Incident, a report to detail:

(a) the nature of the Security Incident;

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

(c) the actions undertaken and length of time taken by the *Contractor* to resolve the Security Incident; and

(d) the actions undertaken by the *Contractor* to prevent recurrence of the Security Incident.

7.6 If there is a suspected security event up to and including a Security Incident, the *Contractor* shall to the extent requested by the TfL CISO (or any duly authorised delegate):

(a) provide information in relation to the Services which is relevant collating, if necessary, relevant information from Sub-contractors' systems and the *Contractor* Personnel;

(b) provide relevant TfL Personnel with supervised access (or, if the Parties agree, direct access) to any relevant systems, *Contractor* Sites and *Contractor* Personnel in order to investigate the security incident; and

(c) follow TfL's directions in relation to the steps necessary or desirable to remedy or protect the integrity of the Services; and

(d) work with TfL to identify any lessons learnt which could mitigate any gaps in process, policy or controls.

and TfL shall reimburse the *Contractor*'s reasonable, demonstrable costs and expenses in relation to the *Contractor*'s compliance with such request.

8. SECURITY LOGGING AND MONITORING

8.1 The *Contractor* shall ensure that the Security Management Plan sets out its monitoring strategy to monitor its own performance of its obligations under this appendix to the Scope. The *Contractor* shall update its monitoring strategy as necessary throughout the *service period* in response to:

(a) changes to applicable laws, regulations and standards;

(b) changes to Good Industry Practice;

(c) any relevant change to the Scope or this appendix to the Scope;

(d) any Security Incident; and

(e) any instruction by the Service Manager.

8.2 The monitoring strategy should include, as a minimum, processes for monitoring and logging (as appropriate):

(a) networks and host systems to detect attacks originating both on an internal private network or from public networks (e.g. internet);

(b) instances of misuse of the Service Assets, *Contractor* systems used in Providing the Services and data by the Parties people, including attempts at such misuse;

(c) wireless access points to ensure that all wireless networks are secure and no unauthorised access points are available;

(d) malicious software on the *Contractor* systems used in Providing the Services and the Service Assets;

(e) access to and movement of Data, including internal access to such Data; and

(f) traffic for unusual or malicious incoming and outgoing activity that could be indicative of an attempt or actual attack.

8.3 The *Contractor* shall ensure that access to system logs and monitoring information is strictly restricted to those people who need to access these to Provide the Service and protest the integrity of the Service Assets.

8.4 The *Contractor* shall ensure that any monitoring process complies with the monitoring strategy developed in accordance with Paragraphs 9.1 and 9.2 and all of its legal and regulatory obligations pursuant to applicable law.

8.5 The *Contractor* shall maintain a log of:

(a) all instances of the *Contractor's* people accessing Data;

(b) all Service Recipient, TfL people and *Contractor* people logon attempts, successful and failed, to the Service Assets or any elements of the *Contractor* Solution requiring authentication;

(c) all actions taken by Service Recipients, TfL people or *Contractor* people with administrative privileges;

(d) all instances of accounts being created for Service Recipients, TfL people or *Contractor* people and their relevant privileges;

(e) all records of formal staff induction or certification required by *Contractor* people to operate systems and handle TFL RESTRICTED Data (where required);

(f) all instances of accounts for Service Recipients, TfL people, or *Contractor* Personnel being deleted;

(g) *Contractor* people system access group memberships in relation to relevant Service Assets;

(h) Service Recipient and group privilege changes against each of the system resources;

(i) unauthorised use of input and output devices and removable media; and

(j) all access to log files and audit systems.

8.6 The logs required must be raw logs, which are provided in a structured text format and the schema for such logs will need to be provided.

8.7 The *Contractor* shall implement recording mechanisms to identify the Parties people and their actions when cases of misuse are being investigated and shall ensure that any such recording mechanisms are protected against manipulation and disruption.

8.8 The *Contractor* shall regularly review logs to identify anomalies, suspicious activity and suspected Security Incidents. The *Contractor* shall notify the Service Manager of such findings in accordance with Paragraph 8.2.

8.9 The *Contractor* shall provide copies of any log data collected by the *Contractor* whilst Providing the Service (system audit log data) at the *Service Manager's* request in a human readable electronic format such as comma-separated value or Microsoft Excel.

9. MALICIOUS SOFTWARE

9.1 The *Contractor* shall throughout the Term, use the latest versions of anti-malware solutions and software available from an industry accepted vendor (unless otherwise agreed by the Service Manager) to check for, contain the spread of, and minimise the impact of Malicious Software in the IT Services.

9.2 Notwithstanding Clause 10.1, if Malicious Software is detected within services provided by the *Contractor*, the *Contractor* shall ensure the effect of the Malicious Software is mitigated and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Data, restore the Service Assets to their desired operating efficiency.

9.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Clause 10.2 shall be borne by the Parties as follows:

(a) by the *Contractor* if the Malicious Software originates from the *Contractor* Software, the Third Party Software supplied by the *Contractor* (except where TfL has waived the obligation set out in Clause 10.11) or TfL Data (whilst TfL Data was under the control of the *Contractor*) unless the *Contractor* can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by TfL when provided to the *Contractor*; and

(b) otherwise by TfL.

10. REMOVABLE MEDIA

10.1 The *Contractor* may only use Removable Media to support Providing the Service if it has obtained prior written consent of the Service Manager 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 Providing the Service.

10.2 If Removable Media is approved for use by the Service Manager, the *Contractor* 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 the Service Manager.

10.3 The *Contractor* shall report any loss or interception of Data as a result of the use of removable media to TfL in accordance with Section 8 of this appendix to the Scope. The *Client* reserves the right in such instances to rescind its approval in relation to the *Contractor*'s continued use of Removable Media.

11. MOBILE AND HOME WORKING

11.1 The *Contractor* may only use offer mobile and home working to support Providing the Service if it has obtained prior written consent of.

11.2 If such consent is granted but the *Contractor* does not have a home and mobile policy for *it's* people, TfL's Home and Mobile Working Cyber Security Policy shall apply to the *Contractor* and its people.

11.3 If the Contractor has a home and mobile working policy in relation to the it's people, the Contractor shall ensure through this policy that:

(a) data is protected and suitably encrypted in line with Cyber Security Policy (see Annex 5), when stored outside of the *service areas*;

(b) data is protected when accessed, imported or exported through a connection other than one which is accessed at the *service areas*; and

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

11.4 The *Contractor* shall report any loss or interception of Data as a result of home or mobile working to the *Service Manager* in accordance with Clause 8.

12. DISPOSALS

12.1 The *Contractor* shall not reuse any Service Asset or Removable Media used in Providing the Service unless such items have been wiped securely in accordance with a standard approved by the *Service Manager*.

12.2 The *Contractor* shall securely dispose of and delete Data from Service Assets used for Providing the Service to a standard approved by the Service Manager upon the termination or expiry of the contract or when such Service Assets are no longer required, whichever is sooner, and shall document the disposal and deletion accordingly.

12.3 The *Contractor* shall ensure that the disposal of any Service Asset is accurately reflected in the Information Asset Register.

13. SECURITY MANAGEMENT PLAN

13.1 The Outline Security Management Plan as at the *starting date* is set out at Annex 1 (*Outline Security Management Plan*).

13.2 The *Contractor* shall within fifteen (15) days of the *starting date* submit to the Service Manager for approval, a draft Security Management Plan which at minimum will:

(a) set out the security measures to be implemented and maintained by the *Contractor* in relation to all aspects of the Service Assets and all processes associated with Providing the Service and shall at all times comply with and specify security measures and procedures which are sufficient to ensure the Service Assets comply with this appendix to the Scope;

(b) reference and comply with the security requirements set out in Annex 3;

(c) state any other cyber security industry standards over and above those set out in this appendix to the Scope which are applicable to the Service Assets or Providing the Service;

(d) state all applicable law which relates to the security of the Service Assets; and

(e) set out how the *Contractor* will comply with any other security requirements the *Client* may reasonably request from time to time.

When the Security Management Plan is approved by the *Service Manager* the approved plan will replace the Outline Security Management Plan in Annex 1.

13.3 The *Contractor* shall review and update the Security Management Plan at least annually and as required in response to:

(a) changes to the Cyber Security Standards;

(b) emerging changes in Good Industry Practice;

(c) any relevant change to the Scope;

(d) any new perceived or changed security threats; and

(e) an instruction by the Service Manager.

13.4 The *Contractor* shall submit any amendments to the Security Management Plan to the Service Manager for approval.

14. INFORMATION SECURITY MANAGEMENT SYSTEM

14.1 The *Contractor* shall develop, implement, operate, maintain the ISMS and shall within fifteen (15) Working Days of the Effective Date submit a draft ISMS to TfL to assure. The *Contractor* shall ensure that the ISMS includes the Security Incident Management Process, dealing with, among other matters, Security Incident management.

14.2 The ISMS shall, unless otherwise specified by TfL in writing, be designed to protect all aspects of:

(a) the Services;

(b) all processes associated with the delivery of the Services; and

(c) TfL Sites, the *Contractor* Solution and any information and Data (including TfL Confidential Information and TfL Data) to the extent used by TfL or the *Contractor* in connection with this Agreement.

14.3 The *Contractor* shall make any document referenced in the ISMS available to TfL upon request.

14.4 If the investigation of a Security Incident reveals weaknesses or flaws in the ISMS, then any change to the ISMS to remedy the weakness or flaw shall be submitted to TfL for approval in accordance with the Variation procedure set out in this Agreement for the avoidance of doubt, if a change needs to be made to the ISMS to address an instance of non-compliance with the Security Management Plan or security requirements, the change to the ISMS shall be at no cost to TfL.

14.5 The ISMS will be fully reviewed in accordance with ISO/IEC 27001 by the *Contractor* at least annually, or from time to time as agreed with TfL, in response to:

(a) changes to Good Industry Practice;

(b) any relevant Operational Changes or Variations or proposed Operational Changes or Variations to the Services and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable request by TfL.

14.6 The *Contractor* shall provide the results of such reviews to TfL (together with such related information as TfL may reasonably request) as soon as reasonably practicable after their completion. The results of the review should include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

(c) proposed modifications to the procedures and controls that affect the ability to respond to events that may impact on the ISMS; and

(d) suggested improvements in measuring the effectiveness of controls.

15. COMPLIANCE WITH ISO/IEC 27001

15.1 The *Contractor* shall obtain certification from a UKAS registered organisation of the ISMS to ISO/IEC 27001 for any aspects of the business that is necessary to support the Services. The *Contractor* shall obtain such certification within twelve (12) months of the Effective Date and shall maintain such certification throughout the Term.

15.2 If certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27001 and Schedule 2.3 (*Standards*) the *Contractor* shall promptly notify TfL of this.

15.3 Without prejudice to any other audit rights set out in this Agreement TfL may carry out, or appoint an independent auditor to carry out, such regular security audits as may be required in accordance with Good Industry Practice in order to ensure that the ISMS maintains compliance with the principles and practices of ISO/IEC27001.

15.4 If on the basis of evidence provided by such audits, TfL, acting reasonably, considers that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the *Contractor*, then TfL shall notify the *Contractor* of the same and the *Contractor* shall, as soon as reasonably practicable, provide TfL with a written plan to remedy each such non-compliance as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement.

16. APPROVED PRODUCTS

16.1 The *Contractor* shall ensure that all Service Assets providing security enforcing functionality are certified under the CESG Commercial Product Assurance (CPA) Scheme, to the appropriate grade, as defined with Annex 3 “Security Requirements”, provided that relevant certified products are available in the market.

16.2 If a product is not assured under the CPA scheme, TfL reserves the right to require bespoke assurance of that product under a recognised scheme such as CESG Tailored Assurance Service (CTAS).

ANNEX 1 – OUTLINE SECURITY MANAGEMENT PLAN/SECURITY MANAGEMENT PLAN

- Not used

ANNEX 2 – OUTLINE RISK MANAGEMENT PROCESS

- Not used

ANNEX 3 – SECURITY REQUIREMENTS

- Not used

ANNEX 4 – CONFIGURATION MANAGEMENT OF SERVICE ASSETS

- Not used

ANNEX 5 – LIST OF RELEVANT POLICIES

TO BE PROVIDED BY TFL UPON REQUEST

- **Network Security Policy** defines the requirements for securing TfL networks as well as the information and network specific devices on them.
- **System Access Control Policy** defines the requirements for managing user and system account access to applications and technology such as allowing them to sign in to OneLondon or SAP.
- **Cyber Security Incident Management Policy** defines how we will handle cyber security incidents and the requirements for reporting and managing those incidents.
- **Malware Prevention Policy** defines the requirements for helping to prevent malware (malicious software e.g. computer viruses) from infecting our systems and networks.
- **Security Logging, Monitoring and Audit Policy** details the requirements for security logging and monitoring of access to our technology and data and the audit capabilities.
- **Removable Media Policy** details the requirements for using removable media such as USBs, CDs or portable hard drives.
- **Home and Mobile Working Cyber Security Policy** details the requirements for allowing and supporting secure home and mobile working.
- **Third Party Cyber Security Policy** defines the rules governing how the security of third party custodians of TfL information, technology and third party connections to TfL systems will be ensured.
- **TfL Information Security Classification Standard** details the information security classification scheme covering information and records, in all formats, and the minimum requirements for managing such information
- **10 Steps to Cyber Security** can be found at https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
- **Cyber Essentials Scheme** can be found at https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
- **Security Patching Standard** details the requirements for applying security-related updates ('security patches') in order to help secure TTL systems and applications in line with the secure builds and configurations policy.
- **Operations Technology Cyber Security Standard** describes the cyber security requirements for operational technology assets throughout their lifecycle