(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 TCL.

15.6 The Contractor shall provide the results of such reviews to TCL (together with such related information as TCL 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.

16. <u>COMPLIANCE WITH ISO/IEC 27001</u>

16.1 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.

16.2 If certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27001 and the Standards the Contractor shall promptly notify TCL of this.

16.3 Without prejudice to any other audit rights set out in this Agreement TCL 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.

16.4 If on the basis of evidence provided by such audits, TCL, acting reasonably, considers that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Contractor, then TCL shall notify the Contractor of the same and the Contractor shall, as soon as reasonably practicable, provide TCL 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.

17. <u>APPROVED PRODUCTS</u>

17.1 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.

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

NG

ANNEX 1 – OUTLINE SECURITY MANAGEMENT PLAN/SECURITY MANAGEMENT PLAN

This will be provided by the Contractor before the final approval of the design of the Devices by TCL.

ANNEX 2 – OUTLINE RISK MANAGEMENT PROCESS

This will form part of the security management plan at annex 1*:*

- How and when risk assessments are conducted
- Once found, what are the timeframes mitigations of risks once discovered
- Whether vulnerability scans or vulnerability management are to be provided
- The regularity of vulnerability scans and penetration testing
- The type of scans required (credentialed or non-credentialed)
- The output of this service- whether the automated report from the scanning tool or a fully analysed report
- Against what baseline the scans will be performed

ANNEX 3 – SECURITY REQUIREMENTS

None

ANNEX 4 – CONFIGURATION MANAGEMENT OF SERVICE ASSETS

None

ANNEX 5 – LIST OF RELEVANT POLICIES

TO BE PROVIDED BY TCL UPON REQUEST

Network Security Policy defines the requirements for securing TCL 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 eg 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 TCL information, technology and third party connections to TCL systems will be ensured.

NB

TCL 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 - https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

Cyber Essentials Scheme 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

NB

SECTION 11

SCHEDULE 11

Permitted Sub contractors

[redacted]

SECTION 12

SCHEDULE 12

List of Third Party Software

[redacted]

Note: Other software as determined during detailed design.

SECTION 13

SCHEDULE 13

Governance

Monthly – Sandilands Programme Steering Group.

This meeting is chaired by the Director of London Trams with attendees being formed of stakeholders appropriate to the subject matter of the meeting, including the Contractor if required.

The monthly Sandilands Programme Steering Group provides overall governance to the Post Sandilands Asset Modification Programme, of which PPOS delivery forms a single work stream. Issues escalating from the Weekly PPOS Project Progress Review will be decided by the Sandilands Programme Steering Group.

Weekly – Project Progress Review.

This meeting is chaired by the LT PPOS Project Manager, and is intended to address all aspects of the delivery and contract management of the PPOS project. The Contractor will compile a weekly progress report addressing the meeting agenda items for presentation to the LT project Manager at the meeting.

The agenda for the meeting will be broadly as follows, but can be amended as required to reflect the subject matter of the meeting:

1. HSQE
2. Project Schedule & Progress Update
3. Technical & Safety Assurance
4. Resource
5. Risks & Opportunities
6. Commercial
7. AOB

Subject to Contractor performance and mutual agreement, this meeting may be amended to bi-weekly.

SECTION 14

SCHEDULE 14

Contractor Confidential Information

[redacted]

NB