Transport for London

Revenue Collection Services

Schedule 9.4 – Security Management

TfL RESTRICTED
Restricted to: TfL Group, Contractor Group and Consultants with NDA

Contents

1 Introduction

1.1 Scope and Purpose

1.1.1 Information security is the preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

1.1.2 This Schedule 9.4 (Security Management) sets out the requirements for the Contractor to establish, implement, operate, monitor, review, maintain and improve a documented Information Security Management Systemwhich shall take into account, amongst other things, TTL's overall business activities and the risks TTL faces. In complying with its obligations under this Schedule, the Contractor shall use a process based on the "Plan-Do-Check-Act" ("**PDCA**") model described in ISO 27001 and summarised in paragraph 1.1.5 below.

1.1.3 The ISMS shall be documented by the Contractor in a document set which shall, as a minimum, comprise the Documents listed in Appendix 1.

1.1.4 The Contractor shall ensure that the ISMS takes, as inputs, the information security requirements set out in this Schedule and the relevant Standards listed in the Schedule 9.3 (Standards). The Contractor shall implement actions and processes to achieve information security outcomes that meet such requirements.

1.1.5 The table below summarises the PDCA model.

Plan **(establish the ISMS)**	Establish Information Security Policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organisation's overall policies and objectives.
Do **(implement and operate the ISMS)**	Implement and operate the Information Security Policy, security controls, processes and procedures.
Check **(monitor and review the ISMS)**	Assess and, where applicable, measure process performance against Information Security Policy, objectives and practical experience and report the results to management for review.
Act **(maintain and improve the ISMS)**	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other activities.

PDCA model applied to ISMS processes

1.1.6 The Contractor shall adopt a collaborative approach with TTL, Related Contractors and Interfacing Parties in defining, implementing, operating, monitoring and improving the ISMS.

1.1.7 The purpose of the Documents to be developed by the Contractor pursuant to this Schedule is to provide Assurance in accordance with Schedule 10.5 (Assurance) to

TTL that the Contractor has arrangements and processes in place that will protect the interests of TTL and TTL Personnel, its agents, the Contractor, the Contractor's Personnel and Customers arising from any security threat and/or Information Security Incident.

1.1.8 The Contractor shall maintain and update the ISMS Documentation throughout the Term and, without limitation to the Contractor's other obligations under this Contract, shall as a minimum address the security of the following areas that fall within the scope of the Services provided by the Contractor:

(a) people;

(b) equipment;

(c) property (including Third Party's property);

(d) information; and

(e) Data (including financial data).

1.1.9 As at the Date of Contract, TTL has achieved compliance for the parts of the System within the scope of PCI-DSS assessment with the requirements of:

(a) the PCI-DSS, Requirements and Security Assessment Procedures, version 2, Oct 2012;

(b) Part K of the Payment Card Industry PIN Transaction Security Point of Interaction, Modular Security Requirements, version 3.0, April 2010; and

(c) the Payment Card Industry Point-to-Point Encryption, Solution Requirements and Testing Procedures Encryption, Decryption, and Key Management within Secure Cryptographic Devices, version 1.1, April 2012,

and the Contractor shall perform its obligations under the Contract in a manner which enables TTL to maintain such compliance and the Contractor shall not through any act or omission compromise such compliance. Where compliance with a later version of such standards is required by TTL, this shall be achieved through Variation. Where the Contractor identifies that an action is required on a Related System and/or Interfacing System in relation to compliance with the PCI-DSS, the Contractor shall notify TTL and provide advice on the proposed solutions, mitigation actions and other actions as may be required by TTL or Third Parties from time to time.

1.1.10 At the Date of Contract, the scope of PCI-DSS is defined by the NCC Group Report on Compliance documents entitled "Point to Point Encryption assessment Report on Compliance (RoC) for Transport for London, Initial Bus Launch", v2.0 (Client Issued), NCC, 13 Nov 2012" and NGSS "PCI Data Security Standard (PCI DSS) Report on Compliance (RoC) for TfL on the Cubic back office IBL Solution", v2.1 (Client Issued), 28 Nov 2012".

2 Establishing and Managing the ISMS

2.1 Establish the ISMS

2.1.1 The Contractor acknowledges the high priority that TTL places on security of Personnel, agents, Customers, contractors, information systems, premises and work sites and the Contractor shall prepare the ISMS Documentation in accordance with this Schedule and shall take into account the provisions of the existing security policy and plans as set out in Appendix 2 (references 'FTA SP' and 'FTA MISP').

2.1.2 For the purposes of Assuring TTL in respect of the ISMS, the Contractor shall:

(a) on the Service Commencement Date, define and document for TTL review and Assurance in accordance with the Submissions Procedure the scope and boundaries of the ISMS in terms of the characteristics of the business, TTL, Sites Assets and technology, and including details of and justification for any exclusions from the scope. Thereafter the Contractor shall review, maintain and submit to TTL for review and Assurance the aforementioned Documents at such times as may be specified by TTL from time to time. For the avoidance of doubt, this scope analysis shall include the System and IRC System, its modules and the Interfaces specified in Schedules 9.1 (Technical Authority) and 7.3 (System Interfaces). If the Contractor deems the application of particular security controls to be inappropriate (e.g. such security control is deemed unnecessary or disproportionate) then prior to the exclusion of such security controls the Contractor shall first be required to justify such exclusion to TTL in writing to TTL's reasonable satisfaction. Where any security controls are excluded, claims of conformity to ISO 27001 shall not be acceptable unless such exclusions do not affect the Contractor's ability, and/or responsibility, to provide information security that meets the security requirements determined by Security Risk assessment in accordance with this Contract and applicable legal or regulatory requirements;

(b) define an Information Security Policy in terms of the characteristics of the business, TTL, Sites, Assets and technology that:

(i) includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security;

(ii) takes into account business and legal or regulatory requirements, Standards, and security obligations set out under, or agreed pursuant to, this Contract;

(iii) aligns with TTL's strategic risk management context in which the establishment and maintenance of the ISMS will take place;

(iv) establishes criteria against which Security Risk will be evaluated (in accordance with paragraph 2.1.2(c)); and

(v) has been Assured;

(c) define a security risk assessment approach consistent with the Security Risk management principles established in Schedule 11.2 (Risk Management) and including:

(i) identification of a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements (the "**Security Risk Assessment Methodology**");

(ii) development of criteria for accepting risks and identification of the levels of Security Risk acceptable to TTL; and

(iii) the Security Risk assessment methodology selected which shall ensure that Security Risk assessments produce comparable and reproducible results;

(d) identify the Security Risks including:

(i) identification of the Assets within the scope of the ISMS, and the owners of those Assets;

(ii) identification of the threats to those Assets;

(iii) identification of the vulnerabilities that might be exploited by such threats to Assets; and

(iv) identification of the impacts that losses of confidentiality, Data, integrity and availability may have on the Assets;

(e) analyse and evaluate the Security Risks including:

(i) assessment of the business impacts upon TTL that might result from Information Security Incidents, taking into account the consequences of a loss of confidentiality, Data, integrity or availability of the Assets;

(ii) assessment of the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these Assets, and the security controls currently implemented;

(iii) estimate of the levels of Security Risks (and the Contractor shall liaise with TTL to ensure that acceptable definitions of levels of Security Risk are used); and

(iv) determination of whether the Security Risks are acceptable or require treatment using the criteria for accepting Security Risks established pursuant to paragraph 2.1.2(c) above;

(f) identify and evaluate options for the treatment of Security Risks (the "**Security Risk Treatment Plan**"). Possible options for the treatment of Security Risks shall include (but shall not be limited to):

(i) applying appropriate security controls;

(ii) knowingly and objectively accepting Security Risks, providing they clearly satisfy TTL’s policies and the criteria for accepting Security Risks (as defined pursuant to paragraph 2.1.2(c) above);

(iii) avoiding Security Risks; and

(iv) transferring the associated business Security Risks to other parties (e.g. insurers, other suppliers, etc);

(g) select security control objectives and security controls for the treatment of Security Risks. Security control objectives and security controls shall be selected and implemented by the Contractor to meet the requirements identified by the Security Risk assessment and Security Risk treatment process for the System and the Contractor shall advise on security control objectives and security controls for the IRC System;

(h) submit to TTL's Information Security Manager for Assurance in accordance with Schedule 10.5 (Assurance) the outcome of the Security Risk evaluation and associated proposed treatment plan described in paragraphs 2.1.2(e) to 2.1.2(g);

(i) develop, submit to TTL for Assurance and maintain on a continuing basis a Security Risk status report which shall include, as a minimum, the information set out in Schedule 11.2 (Risk Management);

(j) summarise the treatment plan for Security Risks categorised as medium,high or very high in the Security Risk status report and ensure that these are ratified by the ISF in the presence of the TCM and the Director of the Contractor responsible for service operations;

(k) prepare a statement detailing the application of security objectives and security controls and which shall include a summary explanation of the treatment of Security Risks which support the application of security controls and security objectives (the "**Statement of Applicability**"). Such statement shall include the following:

(i) the security control objectives and security controls selected in 2.1.2 (g) and the reasons for their selection;

(ii) the security control objectives and security controls currently implemented pursuant to paragraph 2.1.2(e) above;

(iii) the exclusion of any security control objectives and security controls and the justification for their exclusion; and

(iv) a matrix providing traceability and mapping of the security controls with the System, Domains, Module Groups, Modules, Components and Interfaces identified in Schedules 9.1 (Technical Authority) and 7.3 (System Interfaces) (the "**Security Controls Matrix**"). The Security Controls Matrix shall be reviewed during the ISF meetings;

(l) submit the ISF terms of reference to TTL for Assurance within thirty (30) Business Days of the Service Commencement Date;

(m) appoint an Information Security Manager whose responsibilities shall be substantially in the form of the terms of reference included in Appendix 3;

(n) confirm the appointment of the Contractor's Information Security Manager on the Service Commencement Date and shall promptly inform TTL's Information Security Manager of any subsequent changes;

(o) on the Service Commencement Date categorise Information Security Incident types into minor, significant, and major and submit the criteria for each type to TTL for TTL's Information Security Manager's review and Assurance. Following the Service Commencement Date, the Contractor shall review, maintain and submit to TTL for review and Assurance the categories of Information Security Incident types in advance of each Information Security Forum and following the identification of any new Information Security Incident types, a Change, a Variation or following an Information Security Event;

(p) liaise closely with TTL's Information Security Manager regarding any matter arising from the Contractor's ISMS Documentation that impinges on other TTL operations, agents, Third Parties, TTL Personnel and Customers; and

(q) define how to measure the effectiveness of the selected security controls or groups of security controls and specify how these measurements are to be used to assess security control effectiveness to produce comparable and reproducible results.

2.1.3 TTL shall:

(a) keep the Contractor informed on security matters that might have a material impact on the Contractor's ISMS Documentation and operations; and

(b) provide feedback on deliverables submitted by the Contractor in accordance with the procedure set out in Schedule 11.1 (Document Management).

2.2 Implement and operate the ISMS

2.2.1 The Contractor shall:

(a) formulate a Security Risk treatment plan, as part of the ISMS document set described in Appendix 1, that identifies the appropriate management action, resources, responsibilities and priorities for managing information security Security Risks;

(b) implement the Security Risk treatment plan described in paragraph 2.2.1(a) in order to achieve the identified security control objectives, which includes consideration of funding and allocation of roles and responsibilities;

(c) implement and execute security controls on the System which are selected in accordance with paragraph 2.1.2(k) above to meet the security control objectives and in particular to:

(i) promptly detect errors in the results of business-as-usual processing;

(ii) promptly identify attempted and/or successful security breaches and Information Security Incidents; and

(iii) detect Information Security Events and thereby prevent Information Security Incidents by the use of indicators.

The Contractor shall advise TTL on the implementation and execution of security controls on the IRC System.

For the purposes of this Schedule, security controls shall include, but not be limited to, Vulnerability Scanning, anti virus measures, intrusion detection, access control and Penetration Testing activities. The Contractor shall ensure that Penetration Testing is carried out by independent experts specifically contracted for this purpose and results in a Penetration Testing report being produced by such independent experts;

(d) submit outputs of security control execution activities to TTL for Assurance in accordance with Schedule 10.5 (Assurance);

(e) maintain the security controls up to date by taking into account the normal evolution of the external security environment and standards and shall provide a report to TTL on the same (the "**Security Environmental Report**"). The Contractor shall advise TTL as appropriate on the maintenance of security controls in relation to the IRC System;

(f) implement necessary maintenance actions to address Security Risks outlined by activities such as Penetration Testing, Vulnerability Scanning, firewall rules audits, intrusion detection, access control, file integrity management, database audit logs, website audit logs and taking into account vendors' (i.e. those suppliers of maintenance tools) recommendations and shall advise TTL as appropriate on the implementation of necessary maintenance actions in relation to the IRC System;

(g) implement training and awareness programmes for TTL Personnel, Contractor Personnel and Sub-Contractor staff as necessary;

(h) manage the operation of the ISMS;

(i) manage the resources for the ISMS;

(j) implement procedures and other security controls on the System which are capable of enabling prompt detection of Information Security Events and response to Information Security Incidents; and

(k) make arrangements for liaison with external security bodies such as the British Transport Police as required.

2.2.2 The Contractor shall discuss the treatment of Security Risks resulting from major evolution of the security landscape such as breach of standard cryptographic algorithm (RSA, AES etc.) or change of regulation with TTL. Any resulting Changes shall be subject to Variation and implemented in accordance with Schedule 9.1 (Technical Authority) (for Technical Changes), Schedule 10.1 (Change Management), Schedule 10.5 (Assurance) and Schedule 12.3 (Contract Variation Procedure).

2.2.3 The Contractor shall prepare and submit to TTL's Information Security Manager an information security report after each Information Security Incident or each Information Security Event. The Contractor shall notify TTL within one (1) hour of detection of an Information Security Incident or an Information Security Event and shall provide the information security report to TTL within forty-eight (48) hours of the incident or event being detected. The information security report shall include as a minimum:

(a) the date and time of the Information Security Incident or the Information Security Event (as appropriate);

(b) a description of the Information Security Incident or the Information Security Event (as appropriate) including where it occurred or what Sites were affected;

(c) the category type of the Information Security Incident (for example minor, significant, major) or the Information Security Event (as appropriate);

(d) the Domains, Module Groups, Modules, Components and Interfaces (as set out in Schedules 9.1 (Technical Authority) and 7.3 (System Interfaces)) affected;

(e) the nature of security breach;

(f) the actions taken as a result;

(g) details of the impact on the Contract (e.g. milestones, objectives, administration, payments, availability);

(h) the lessons learnt; and

(i) details of proposed amendments to procedures and processes to prevent recurrence or similar incidents or events.

2.2.4 TTL shall:

(a) review the information security reports and provide feedback to the Contractor; and

(b) consider with the Contractor any proposed amendments to procedures and processes and decide whether they should be implemented and, if so, within what timeframe.

2.2.5 The Contractor shall maintain an information security log recording all Information Security Incidents and Information Security Events and the actions taken as a result (the "**Security Log**"). The Security Log shall be capable of being sorted and presented by:

(a) Domains, Module Groups, Modules, Components and Interfaces;

(b) Information Security Incident type or Information Security Event type (as appropriate); and

(c) date of Information Security Incident or Information Security Event (as appropriate).

2.3 Information Security Forum

2.3.1 The purpose of the information security forum is to review and address any matters relating to the ISMS and/or security and to ensure that there is clear direction and visible Contractor management support for information security initiatives in accordance with this paragraph 2.3 (the "**Information Security Forum**" or "**ISF**").

2.3.2 The Contractor shall prepare the meeting agenda for each ISF and the Contractor's Information Security Manager shall chair the meeting. At the end of each ISF meeting there shall be an agreed set of actions and the Contractor shall produce formal minutes that shall be circulated within three (3) Business Days of each meeting.

ATTENDEES		
TTL	**Contractor**	**Third Parties**
TTL's Information Security	Contractor's Information	Any representative of a Related Contractor or

Copyright Transport for London 2014

Manager Any other representative of TTL relevant to the matters to be discussed at the meeting	Security Manager Any other representative of the Contractor relevant to the matters to be discussed at the meeting	Interfacing Party relevant to the matters to be discussed at the meeting

FREQUENCY AND LOCATION
Once each Period or upon the reasonable request of either TTL or the Contractor. In London at a location agreed by TTL.

CONTRACT MANAGEMENT ROLE	
Review of last meeting	• The Parties shall review and approve the previous ISF meeting minutes and action log (if applicable) • TTL shall notify the Contractor if it deems any outstanding actions in the action log to be closed (otherwise, such actions shall remain open until closed by TTL and notified to the Contractor in writing)
General	The objectives of the ISF are to: • oversee, review information security policies, the ISMS, practices and responsibilities • review, Assure and monitor Information Security Events and Information Security Incidents • review security audits reports and monitor implementation of follow up actions • review the Security Controls Matrix and ensure it is accurate and representative of the System • provide Assurance in accordance with Schedule 10.5 (Assurance) that Security Risk activities described in paragraph 2.1.2 of this Schedule have been conducted during implementation of Changes in accordance with Schedule 10.1 (Change Management) • review changes to Standards and their impact on ISMS • provide technical recommendations to developments within the System and to the IRC System to ensure the confidentiality, integrity and availability of the information System and/or the IRC System

INPUTS AND OUTPUTS	
Required Inputs	• Previous ISF meeting minutes and action log

	• Details of Information Security Events and Information Security Incidents • Security Controls Matrix • The Security Log • Audit reports • Risk status report (as required by Schedule 11.2 (Risk Management))
Required Outputs	Updated action log

2.3.3 TTL's Information Security Manager shall have the right to convene specific meetings to discuss serious incidents and breaches of security or to brief the Contractor on security matters initiated within TTL and having an impact on the Contractor's ISMS Documentation. The Contractor shall attend all such meetings.

2.4 Monitor and Review the ISMS

2.4.1 The Contractor shall:

(a) measure the effectiveness of security controls to verify that security requirements have been met;

(b) undertake annual reviews of the effectiveness of the ISMS (including meeting Information Security Policy and objectives, and review of security controls) taking into account results of security audits, Information Security Incidents, Information Security Events, results from effectiveness measurements, suggestions and feedback from all Interested Parties;

(c) enable TTL to determine whether the security activities and associated security controls are performing as expected;

(d) following an Information Security Event, review, determine and document whether the actions taken to resolve a breach of security were effective and submit such Document to TTL for Assurance;

(e) conduct Security Risk assessment activities described in paragraph 2.1.2 of this Schedule, taking into account changes to:

(i) TTL Group;

(ii) technology;

(iii) business objectives and processes;

(iv) identified threats;

(v) effectiveness of the implemented security controls; and

(vi) external events, such as changes to the legal or regulatory environment, changes to external threats environment, changed contractual obligations in accordance with this Contract, and changes in social climate;

(f) conduct internal monthly rolling ISMS audits in accordance with paragraph 2.5.1 below;

(g) undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified (see paragraph 2.6 below);

(h) produce a security improvement plan which sets out the Contractor's proposals for improving security controls and security objectives ("**SIP**") for TTL review and Assurance leading to the updating of the security framework of the ISMS to take into account the findings of monitoring and review activities; and

(i) record actions and events that could have an impact on the effectiveness or performance of the ISMS.

2.4.2 The Contractor shall pro-actively keep abreast of Standards that are modified or introduced and flag relevant changes at the ISF meetings for consideration in the ISMS improvements.

2.4.3 The Contractor shall review, maintain and advise on security controls on a continuing basis. The Contractor shall ensure that a formal review of security controls is undertaken at least once per Contract Year and shall provide a report on the same to TTL for Assurance.

2.4.4 The Contractor shall, as part of its continuing review and formal review of security controls, propose pre-emptive changes to such security controls as they become necessary to respond to new security threats and other changes. The Contractor shall ensure that its proposed plan to implement such proposed changes is cost-effective and minimises risk. Where the Contractor reasonably proposes changes to any of the following, and such proposals have not arisen as a result of a failure by the Contractor to comply with its obligations under the Contract, they shall be considered by TTL. If TTL requires proposed changes to the following to be implemented, TTL shall instruct the Contractor through the Variation Procedure:

(a) the Card technology platform (e.g. MiFare DESFire);

(b) cryptographic key rollover periods;

(c) cryptographic key lengths;

(d) cryptographic algorithms (e.g. 3DES to AES or RSA to ECC);

(e) firewall Software; or

(f) networking Software.

2.5 ISMS rolling audit

2.5.1 The Contractor shall conduct an internal ISMS monthly rolling audit to determine whether the security control objectives, security controls, processes and procedures of the ISMS maintained by the Contractor pursuant to this Schedule conform to ISO27001.

2.5.2 Each month the Contractor shall conduct an audit on a part of the ISMS resulting in an interim audit report at the end of each month and a consolidated report at the end of the Contract Year.

2.5.3 The Contractor shall propose to TTL for TTL's approval a competent Third Party to conduct an ISO 27001 audit three (3) times during the Term (such audits at the sole cost of the Contractor), the specific times to be agreed between TTL and the Contractor at the end of each Contract Year.

2.5.4 All audit reports produced in accordance with this paragraph 2.5 shall be submitted to TTL for Assurance in accordance with Schedule 10.5 (Assurance).

2.6 Management review overview

2.6.1 The Contractor's Director responsible for service operations shall review the Contractor's ISMS once per Contract Year to ensure its continuing suitability, adequacy and effectiveness (a "**Management Review**"). This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the Information Security Policy and information security objectives. The results of the reviews shall be clearly documented and records shall be maintained in accordance with paragraph 2.8 of this Schedule and shall be available upon request by TTL.

2.6.2 The input to a Management Review by the Contractor shall include:

(a) results of ISMS audits and reviews conducted pursuant to paragraph 2.5.1 of this Schedule;

(b) feedback from Interested Parties;

(c) techniques, products or procedures, which could be used to improve the ISMS performance and effectiveness;

(d) status of preventive and corrective actions;

(e) vulnerabilities or threats not adequately addressed in the previous Security Risk assessment (both newly discovered and previously known but not considered adequately addressed at this time);

(f) results from effectiveness measurements;

(g) follow-up actions from previous Management Reviews;

(h) any changes that could affect the ISMS; and

(i) recommendations for improvement of the ISMS.

2.6.3 The output from the Management Review shall include any decisions and actions by the Contractor related to the following:

(a) improvement of the effectiveness of the ISMS;

(b) update of the Security Risk assessment and Security Risk treatment plan;

(c) modification of procedures and security controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:

(i) business requirements;

(ii) security requirements;

(iii) business processes effecting the existing business requirements;

(iv) regulatory or legal requirements;

(v) contractual obligations; and

(vi) levels of Security Risk and/or criteria for accepting Security Risks;

(d) resource needs; and

(e) improvement to how the effectiveness of security controls is being measured.

2.6.4 The output from the Management Review described in paragraph 2.6.3 above shall be submitted to TTL for review and Assurance within ten (10) Business Days of the Management Review meeting.

2.7 Maintain and improve the ISMS

2.7.1 The Contractor shall, at least annually:

(a) implement ISMS improvements (identified as part of the monitoring, review, audit and Management Review processes set out in this Schedule and documented in the SIP. The Contractor shall continually improve the effectiveness of the ISMS through the use of the Information Security Policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and Management Review;

(b) take appropriate corrective and preventive actions (which shall be specifically identified in the SIP) as detailed below in this paragraph including applying the lessons learnt from the security experiences of other organisations and those of TTL itself:

(i) ***Corrective actions***: The Contractor shall take action to eliminate the cause of non-conformities with the ISMS requirements in order to prevent recurrence. The Contractor's documented procedure for corrective action shall define requirements for:

- identifying nonconformities;
- determining the causes of nonconformities;
- evaluating the need for actions to ensure that nonconformities do not recur;
- determining and implementing the corrective action needed;
- recording results of action taken; and
- reviewing any corrective action taken;

(ii) ***Preventative actions***: The Contractor shall determine action to eliminate the cause of potential non-conformities with the ISMS requirements in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The Contractor shall identify changed Security Risks and preventive action requirements focusing attention on significantly changed Security Risks. The priority of preventive actions shall be determined based on the results of the Security Risk assessment. The Contractor's documented procedure for preventive action shall define requirements for:

- identifying potential nonconformities and their causes;
- evaluating the need for action to prevent occurrence of nonconformities;
- determining and implementing preventive action needed;
- recording results of action taken; and
- reviewing any preventive action taken;

(c) communicate the actions and improvements to all Interested Parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed; and

(d) ensure that any improvements made to the ISMS achieve their intended objectives.

2.8 Documentation requirements

2.8.1 The Contractor shall produce and submit to TTL for Assurance in accordance with Schedule 10.5 (Assurance) the Documents listed in Appendix 1 to this Schedule within the timeframes set out in that Appendix.

2.8.2 The Contractor shall submit to TTL's Information Security Manager a comprehensive and up-to-date list of the Documents published related to the security of the System and the IRC System (the "**Security Documentation Log**").

2.8.3 Documentation to be produced by the Contractor for TTL review pursuant to this Schedule 9.4 (Security Management) shall include records of management decisions and the Contractor shall ensure that actions are traceable to management decisions and policies.

2.8.4 The Contractor shall maintain Documentation that is able to demonstrate the relationship from the selected security controls back to the results of the Security Risk assessment and Security Risk treatment process, and subsequently back to the Information Security Policy and objectives.

2.8.5 TTL shall make available copies of the relevant sections of relevant existing Documents such as its security policy and relevant security plans and requirements (such Documents as set out in Appendix 2) in connection with the Contractor's preparation of the ISMS Documentation required by this Schedule.

2.8.6 The Documents summarised in Appendix 1 shall be submitted by the Contractor’s Information Security Manager to TTL’s Information Security Manager. Appendix 1 sets out what information needs to be documented, which Documents the content should be contained in, similar documents existing as at the Service Commencement

Date and the frequency with which each Document should be reviewed and considered for revision.

2.8.7 For clarification, where the term "documented procedure" appears within this Schedule, this means that (i) the procedure is established, documented, implemented and maintained; and (ii) Documents and records may be in any reasonable written form or type of medium.

2.9 Working with Third Parties

2.9.1 The Contractor shall work co-operatively towards the common goals of the ISMS with Third Parties nominated by TTL, including:

(a) Qualified Security Assessor (QSA): the organisation that has been qualified by the Payments Council to have their employees assess compliance to the PCI-DSS standard;

(b) Merchant Acquirer: the organisation which acquires the payment card transactions for TTL by processing settlement requests, charge-backs, etc. e.g. Barclays; and

(c) Payment Schemes: the organisation that provide credit and debit payment networks, e.g. Visa, MasterCard and American Express.

3 Management Responsibility

3.1 Management Commitment

3.1.1 The Contractor's management team shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

(a) establishing an Information Security Policy;

(b) ensuring that ISMS objectives and plans are established;

(c) establishing roles and responsibilities for information security;

(d) communicating to the Contractor's organisation and TTL the importance of meeting information security objectives and conforming to the Information Security Policy, its responsibilities under applicable Law and the need for continual improvement;

(e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (as further set out in paragraph 3.2);

(f) deciding the criteria for accepting Security Risks and the acceptable levels of Security Risk;

(g) ensuring that internal ISMS audits are conducted (as further set out in paragraph 2.5.1); and

(h) conducting management reviews of the ISMS (as further set out in paragraph 2.6).

3.2 Provision of Resources

3.2.1 The Contractor shall determine and provide suitably qualified, competent and experienced resources needed to:

(a) establish, implement, operate, monitor, review, maintain and improve the ISMS;

(b) ensure that information security procedures support the business requirements;

(c) identify and address legal and regulatory requirements and security obligations set out in this Contract;

(d) maintain adequate security by correct application of all implemented security controls;

(e) carry out reviews when necessary, and react appropriately to the results of these reviews; and

(f) improve the effectiveness of the ISMS, where required or necessary.

3.3 Training, Awareness and Competence

3.3.1 The Contactor shall ensure that all Contractor Personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

(a) determining the necessary competencies for Contractor Personnel performing work effecting the ISMS;

(b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;

(c) evaluating the effectiveness of the actions taken; and

(d) maintaining records of education, training, skills, experience and qualifications.

3.3.2 The Contractor shall also ensure that all relevant Contractor Personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

Appendix 1 – Documentation Required

In the table below:

- references to source documents are set out with the reference "ref #[●]" which denotes the corresponding item in the table set out in Appendix 2 to this Schedule
- references to "annually" shall mean the anniversary of the Service Commencement Date or such other date as the Parties may agree.

Content needed	***Relevant document***	***Source documents***	***Timeframe for submission to TTL and review frequency***
Plan (establish the ISMS)			
The Contractor shall establish and submit the ISMS Documentation described in this table on the Service Commencement Date which shall include (but shall not be limited to):	ISMS Documentation	Existing ISMS Documentation supplied by TTL (see Appendix 2)	On the Service Commencement Date. Review frequency post the Service Commencement Date Data is given for each individual Document in this table below.
• Documented statements of the Information Security Policy in accordance with paragraph 2.1.2(b) of this Schedule and objectives.		FTA Information Security Policy: ref #10	Annually
• The scope of the ISMS in accordance with paragraph 2.1.2(a).		FTA Security Plan: ref #12	Annually
• Procedures and controls in support of the ISMS.		Ref #9 - Appendix A for examples.	Annually
• A description of the Security risk assessment methodology in accordance with paragraph 2.1(c)(i).		Chyp SRA methodology: ref #2	Annually
• Risk assessment report in accordance with paragraph 2.1.2(c) to (g)).		SRA report for FTP: ref #16	Annually

Content needed	***Relevant document***	***Source documents***	***Timeframe for submission to TTL and review frequency***
Risk treatment plan in accordance with paragraph 2.1.2(f) for managing information security risks which identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks.	Security Risk Treatment Plan	FTP Controls spreadsheet: ref #13; FTA Risk Management Plan: ref #11	Annually
Documented procedures to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of security controls.	Security Procedures	e.g. User Access Control Procedures: Schedule 8.4 (Access Management)	Annually
A description of the security control objectives and security controls selected and which are implemented and why. Provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no security controls have been inadvertently omitted.	Statement of Applicability	FTP Controls spreadsheet: ref #13	Annually
Terms of reference for ISF.	ISF Terms of Reference	FTA ISF Terms of reference: ref #7	Annually
Traceability and mapping of the security controls within the System, Domains, Module Groups, Module, Components and Interfaces	Security Controls Matrix	n/a	Five (5) Business Days before ISF meeting
Do (implement and operate the ISMS)			
ISF meeting minutes	ISF meeting minutes	ISF meeting minutes	Every Period
The Contractor shall submit to TTL's Information Security Manager a comprehensive and up-to-date list of the Documents published related to the security of the System and the IRC System.	Security Documentation Log	Ref #9	Annually
Status Report. Logs of agreed daily monitoring of TTL's systems. The requirement is to report the status regardless of whether there are any Information Security Incidents.	Daily Status report	Daily Status report	Every day

Content needed	***Relevant document***	***Source documents***	***Timeframe for submission to TTL and review frequency***
Information Security Report. Intrusion alerts shall be notified to TTL within one (1) hour of the detected incident.	Security Incident Notifications	N/A	To be notified to TTL within one (1) hour of detection and the report shall be provided to TTL within forty-eight (48) hours of the incident being detected
A Security Log. A record of all Information Security Incidents and the actions taken.	Security Log	N/A	Five (5) Business Days before ISF meeting
Check (monitor and review the ISMS)			
Intrusion and Penetration Detection and Access Controls (in accordance with paragraph 2.4.1)	Intrusion and Penetration Detection report	N/A	Six (6) months from the anniversary of the Service Commencement Date.
New threats and new standards. The Contractor will scan for relevant new threats and standards and will maintain and improve the ISMS accordingly (see paragraph 2.4.1)	Security Environmental report	N/A	Annually
New vulnerabilities in accordance with paragraph 2.2.1. Assess the threat of 'known attacks' in the industry such as from rogue or malicious software. This includes malware and Virus protection.	Vulnerability Assessment report	N/A	Annually
Standards Compliance. The Contractor compiles a list of relevant standards and assesses how compliant the ISMS is with relevant standards.	Standards Compliance report	N/A	Annually
Outcome of ISO27001 rolling audit	Interim Internal ISO 27001 Audit report	Ref #14	Within ten (10) Business Days of each audit
Outcome of ISO27001 rolling audit	Consolidated Internal ISO 27001 Audit report	N/A	Annually
Security Improvement Plan in accordance with paragraph 2.4.1(h))	Security Improvement Plan (SIP) report	N/A	Annually

Appendix 2 – References

This Appendix 2 sets out the references used in this document.

General

This Appendix sets out the reference documents that contain the security requirements which are not contained in this Schedule.

[redacted]

Appendix 3 - Terms of Reference

This section contains the proposed Terms of Reference for the Contractor’s Information Security Manager.

Job Description

Job title: Information Security Manager

Job purpose: To manage the Information Security Management System relating to TTL’s services to Customers and to protect and maintain the availability, integrity, and confidentiality of information Assets.

Key responsibilities:

The Information Security Manager is responsible for ensuring that the aims of Information Security Management are met. This includes such tasks and responsibilities as:

- Developing and maintaining the Information Security Policy and a supporting set of specific policies, procedures and security controls, ensuring appropriate authorisation, commitment and endorsement managers
- Performing security risk analysis and risk management and assisting with Business Impact Analyses
- Performing security tests and managing internal audits on information security processes, security controls and systems
- Developing and documenting procedures for operating and maintaining security controls
- Monitoring and managing all security breaches and handling Information Security Incidents in conjunction with the customer services department
- Preparing the project disaster recovery and business continuity plans for information systems
- Ensuring all changes to services are assessed for impact on all security aspects
- Serving as an internal information security consultant to the Contractor
- Monitoring changes in legislation and accreditation standards that affect information security
- Providing guidance and consultation on projects for IT security related risks and issues
- Liaising with Customers on information security matters for the process of assurance and for compliance to customers' security requirements
- Acting as a single point of contact for Customers on Information Security
- Providing direct information security training to all employees, contractors, and other Third Parties
- Initiating, facilitating, and promoting activities to foster information security awareness among Contractor Personnel

Relationships: Must be able to work effectively and uphold professional standards, with TTL internal and external customers, staff at all levels of the organisation and TTL suppliers and customers.