SCHEDULE 2.4

SECURITY MANAGEMENT

VERSION CONTROL

VERSION NUMBER	DATE	COMMENT
1.0	27 June 2018	Executed by the Parties

CONTENTS

1	PURPOSE	1
2	SECURITY PRINCIPLES	1
3	ACCESS CONTROLS AND SECURE CONFIGURATION OF SYSTEMS	2
4	SUPPLIER PERSONNEL	3
5	TRAINING	3
6	TESTING AND AUDIT	3
7	SECURITY INCIDENT MANAGEMENT PROCESS	5
8	SECURITY LOGGING AND MONITORING	7
9	NOT USED	8
10	REMOVABLE MEDIA	8
11	MOBILE AND HOME WORKING	9
12	DISPOSALS	9
13	SECURITY MANAGEMENT PLAN	9
14	INFORMATION SECURITY MANAGEMENT SYSTEM	10
15	COMPLIANCE WITH ISO/IEC 27001:2013	11
16	APPROVED PRODUCTS	11

APPENDIX 1 – OUTLINE SECURITY MANAGEMENT PLAN

SCHEDULE 2.4 – SECURITY MANAGEMENT

1. PURPOSE

1.1 The purpose of this Schedule is to set out:

1.1.1 the principles of protective security to be applied by the Supplier in performance of this Agreement;

1.1.2 the Supplier's wider security obligations relating to this Agreement;

1.1.3 the Supplier's requirements to test and audit the Services including the ISMS, to ensure compliance with the security requirements set out in this Agreement;

1.1.4 the Supplier's obligations in the event of a Security Incident;

1.1.5 the principles for the Supplier's development, implementation, operation, maintenance and continual improvement of the Security Management Plan;

1.1.6 the principles for the Supplier's development, implementation, operation, maintenance and continual improvement of the ISMS;

1.1.7 the Supplier's obligations for certification against the Services including in relation to ISO/IEC 27001:2013, the Cyber Essentials Scheme and the HMG Information Security Assurance Standards; and

1.1.8 the Supplier's obligation to deliver the Services and Assets in accordance with the CPA Scheme.

2. SECURITY PRINCIPLES

2.1 The Supplier acknowledges that security, data protection and confidentiality are of fundamental importance in relation to its performance of this Agreement and TTL's ability to retain public confidence. The Supplier shall at all times comply with the security principles set out in this paragraph 2 in the performance of this Agreement.

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

2.2.1 appropriate members of Supplier Personnel and the Supplier's management team take responsibility for managing the different levels of security risk and promoting a risk management culture;

2.2.2 a Security Risk Register is produced and maintained throughout the Term and that all Security Risks are documented in an appropriate manner and is included in any contract risk register if one is in place. The Security Risk Register must be available for audit when reasonably required by TTL as set out in paragraph 6;

2.2.3 an Information Asset Register is produced and maintained throughout the Term and that all Assets are documented in an appropriate manner in the Information Asset Register and shall identify the criticality of the relevant Assets in the delivery of this Agreement. This register must be available for audit when reasonably required by TTL as stated in paragraph 6 and when a Security Incident occurs;

2.2.4 supporting policies are implemented (where relevant) and communicated with Supplier Personnel.

2.3 The Supplier shall, and shall procure that its Sub-contractors shall, at all times ensure that:

2.3.1 security threats to the RTO System, the TTL IT Environment and the Services are minimised and mitigated;

2.3.2 the RTO System and the Services shall fully comply at all times with:

(a) the security requirements set out in this Agreement;

(b) the Security Management Plan; and

(c) Good Industry Practice.

2.4 The Supplier shall not (and shall enure that the Sub-contractors shall not) use any Cloud for, or in connection with, the performance of this Agreement (including in relation to any TTL Data) without TTL's prior written approval and, if so provided, the Supplier shall ensure that any such Cloud complies with this Schedule.

3. ACCESS CONTROLS AND SECURE CONFIGURATION OF SYSTEMS

3.1 The Supplier shall comply with all obligations relating to the patching and configuration management of the Assets in accordance with the applicable Standards set out in Schedule 2.3 (Standards) and, in addition, the Supplier shall ensure that:

3.1.1 security patches are applied to the Assets as soon as is possible in line with vendor recommendations in accordance with the Supplier's overall risk management solution;

3.1.2 account management and configuration control processes are implemented to ensure that access to the Assets by Supplier Personnel is limited to the extent required for them to fulfil their roles in supporting the delivery of this Agreement;

3.1.3 when Supplier Personnel change roles or no longer support the delivery of this Agreement access rights are revoked or reviewed;

3.1.4 any system administration functionality is strictly controlled and restricted to those Supplier Personnel who need to have access to such functionality and that the ability of Supplier Personnel to change the configuration of the RTO Sytem and the Services is appropriately limited and fully auditable;

3.1.5 Supplier Personnel are informed of what constitutes acceptable access to Operational Technology or IT systems or services, data and/or networks and the consequences of non-compliance;

3.1.6 any preconfigured passwords delivered with any Assets are changed in accordance with the System Access Control Standard referred to in Schedule 2.3 (Standards) prior to their implementation for use in connection with this Agreement;

3.1.7 the RTO System and the Services have appropriate devices, tools or applications in place to filter traffic or segregate networks, such as industry standard firewalls and Malicious Software protection, to all public or private networks which are not controlled by or on behalf of TTL;

3.1.8 all wireless functionality is appropriately secured in accordance with the System Access Control Standard and the Cryptography Standard (in both cases as referred to in Schedule 2.3 (Standards)); and

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

4. SUPPLIER PERSONNEL

4.1 The Supplier shall appoint a member of Supplier Personnel 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 Agreement. The Security Manager shall be a member of the Key Personnel.

4.2 The Supplier shall ensure that all Supplier Personnel are security screened, cleared or vetted appropriate to the classification of TTL Data that the Supplier Personnel are expected to view and process as part of their role, and shall provide TTL within five (5) Working Days of the Effective Date, and every twelve (12) months thereafter, written confirmation that this obligation has been complied with.

4.3 The Supplier shall immediately notify TTL if it becomes aware of any security clearance issues in relation to the Supplier Personnel and the Supplier shall undertake any action requested by TTL in relation to mitigating the impact of any such security clearance issues.

5. TRAINING

5.1 The Supplier shall ensure that all Supplier Personnel have undergone suitable security awareness training prior to their deployment in connection with this Agreement 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 Supplier shall implement an up-to-date on-going programme of security awareness training for Supplier Personnel throughout the Term.

5.2 The Supplier shall provide additional training to its Supplier Personnel as the relevant circumstances under this Agreement may require from time to time, including following a Security Incident, any relevant Operational Change or Contract Change and prior to the application of a patch or update (including any RTO System Update).

5.3 The Supplier shall ensure that all Supplier Personnel are familiar with their responsibilities under applicable Law and policies including, as a minimum, the Data Protection Laws, the security Standards set out in Schedule 2.3 (Standards) or as otherwise notified by TTL to the Supplier from time to time and policies in relation to the handling of protectively marked materials (as notified by TTL) both during their employment and upon the termination of, or any change to, the terms of their employment.

6. TESTING AND AUDIT

6.1 The Supplier shall conduct regular automated vulnerability scans of the RTO System and the Services, as agreed in the Security Management Plan, and shall ensure that any identified vulnerabilities are appropriately mitigated or patched in accordance with the applicable Standards set out in Schedule 2.3 (Standards), taking into consideration the risk posed to TTL, the RTO System and the Services.

6.2 The Supplier shall be responsible for ensuring that security tests are conducted, including ethical hacking and penetration tests, to assure compliance with the security provisions in this Agreement and the Security Management Plan. Security penetration tests shall be conducted by an independent third party specialist agreed by TTL in writing. The Supplier shall ensure security testing is conducted in accordance with the Security Management Plan. The security tests shall include security penetration testing of the RTO System and the Services and the associated technical infrastructure. Wherever the RTO System and/or the Services are accessible from the internet or other such public network as agreed by TTL in writing, the Supplier shall ensure security penetration tests are carried out from the internet or the public network. The Supplier shall ensure such security tests are conducted:

6.2.1 prior to the Operational Commencement Date in accordance with Schedule 6.1 (Transition); and

6.2.2 at a minimum every twelve (12) months from the Operational Commencement Date and, in addition, as the relevant circumstances under this Agreement may require from time to time.

6.3 The Supplier shall, within five (5) Working Days following completion of the security tests carried out in accordance with paragraph 6.2, provide a report to TTL setting out:

6.3.1 the outcome of such security tests including all identified vulnerabilities;

6.3.2 the Supplier's plans to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement.

6.4 The Supplier shall implement its plans to remedy each identified vulnerability in accordance with the report delivered pursuant to paragraph 6.3 save to the extent directed by TTL in writing.

6.5 Where requested by TTL the Supplier shall following a Security Incident ensure such additional security testing over and above the obligations set out in paragraph 6.2 is carried out as TTL requires.

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

6.7 In addition to its other obligations set out in this Agreement, the Supplier shall at least once during each twelve (12) month period starting from the Operational Commencement Date, engage an appropriately skilled third party to conduct a formal audit of the RTO System and the Services against the then current versions of the following:

6.7.1 the security controls, processes and procedures required pursuant to this Agreement;

6.7.2 the Data Protection Laws (using BS10012 or another standard as agreed with TTL), where applicable; and

6.7.3 the Security Management Plan,

and shall, within five (5) Working Days of becoming aware of actual or potential security issues which impact or could impact the RTO System and/or the Services, inform TTL of each such issue and shall keep TTL up-to-date as the Supplier investigates the nature and impact of such issue. Within five (5) Working Days of the finalisation of the audit findings, the Supplier shall provide to TTL a copy of all such findings which are relevant to the RTO System and/or the Services.

6.8 Without prejudice to any other right of audit or access granted to TTL pursuant to this Agreement or at Law, TTL and/or its representatives may carry out such audits in relation to security matters as are reasonably required to assess the Supplier's compliance with the ISMS and the Security Management Plan.

6.9 If any test or audit carried out pursuant to this paragraph 6 reveals any non-compliance with this Agreement or vulnerability (and, in the case of a TTL audit, TTL has informed the Supplier thereof), the Supplier shall, as soon as reasonably practicable, provide TTL 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 Agreement at the

Supplier's cost. The Supplier shall implement its plans to remedy each identified vulnerability in accordance with such report save to the extent directed by TTL in writing.

7. SECURITY INCIDENT MANAGEMENT PROCESS

7.1 The Supplier shall, and shall ensure that its Sub-contractors shall:

7.1.1 establish, document and share with TTL within the Security Incident Management Process to identify and respond to Security Incidents and mitigate the impact of such Security Incidents on the RTO System and the Services, including in relation to assigning clearly defined roles and responsibilities to specific Supplier Personnel;

7.1.2 record each Security Incident and corresponding Severity Level in the Supplier's ISMS; and

7.1.3 without limitation to the other provisions of this Agreement, follow TTL's reasonable instructions in relation to the identification and resolution of any Security Incident.

7.2 The Supplier shall notify TTL as soon as possible and in any event no later than within one (1) hour upon becoming aware of any Security Incident or any potential Security Incident.

7.3 In addition to the requirements in paragraph 7.2, the Supplier shall additionally provide written notice with all relevant details reasonably available of any actual or suspected breach of security in relation to TTL Personal Data including unauthorised or unlawful access or Processing of, or accidental loss, destruction or damage of any TTL Personal Data.

7.4 If a Security Incident occurs, the Supplier shall, within the framework of the Security Incident Management Process:

7.4.1 immediately take steps to assess the scope of the TTL Data, user accounts and/or TTL Personal Data compromised or affected including, but not limited to, the amount of TTL Data and/or TTL Personal Data affected;

7.4.2 immediately take the steps necessary to remedy or protect the integrity of the RTO System and the Services against any such Security Incident;

7.4.3 securely collect and preserve evidence, including logs, to support the Security Incident Management Process and share with TTL such evidence via secure channels as requested by TTL;

7.4.4 handle any information pertaining to the Security Incident according to the handling requirements for TTL RESTRICTED information defined in TTL's Information Security Classification Standard listed in Schedule 2.3 (Standards);

7.4.5 promptly escalate the Security Incident to a person or governance forum with a level of seniority within the Supplier's organisation as TTL may reasonably require;

7.4.6 as requested by TTL:

(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 Supplier Personnel);

(b) provide relevant TTL Personnel with supervised access (or, if the Parties agree, direct access) to any relevant systems, Supplier Sites and Supplier Personnel in order to investigate the Security Incident;

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

(d) as soon as reasonably practicable develop and provide TTL 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 Supplier to:

(i) correct, make good, reinstate, replace and remediate all deficiencies and vulnerabilities, loss and/or damage to the TTL Data, the RTO System and/or Services in connection with the Security Incident; and

(ii) perform or re-perform any security tests or alternative tests relating to the security of the Assets, the RTO System and/or the Services as appropriate and within the timescales specified by TTL, to assure TTL that the Security Incident has been addressed and its effects mitigated,

provided that any such remediation must be implemented in accordance with this Agreement. The Supplier shall fully implement and comply with such remediation plan save to the extent directed by TTL in writing.

7.5 The Supplier shall provide a detailed report to TTL within two (2) Working Days of the resolution of the Security Incident, such report to detail:

7.5.1 the nature of the Security Incident;

7.5.2 the causes and consequences of the Security Incident;

7.5.3 the actions undertaken and length of time taken by the Supplier to resolve the Security Incident; and

7.5.4 the actions undertaken by the Supplier to prevent recurrence of the Security Incident.

7.6 If there is a suspected security event up to and including a Security Incident the Supplier shall, to the extent requested by TTL's Chief Information Security Officer (or any duly authorised delegate):

7.6.1 provide information in relation to the RTO System, the Assets and the Services which is relevant collating, if necessary, relevant information from Sub-contractors' systems and the Supplier Personnel;

7.6.2 provide relevant TTL Personnel with supervised access (or, if the Parties agree, direct access) to any relevant systems, Supplier Assets, Supplier Sites and Supplier Personnel in order to investigate the security event;

7.6.3 follow TTL's directions in relation to the steps necessary or desirable to remedy or protect the integrity of the RTO System, the Assets and the Services; and

7.6.4 work with TTL to identify any lessons learnt which could mitigate any gaps in process, policy or controls,

and (save where the security event is caused, or contributed to, by a Default by the Supplier) TTL shall reimburse the Supplier's reasonable, demonstrable costs and expenses in relation to the Supplier's compliance with such request.

8. SECURITY LOGGING AND MONITORING

8.1 The Supplier shall ensure that the Security Management Plan sets out the Monitoring Strategy to monitor its own performance of its obligations under this Schedule. The Supplier shall update the Monitoring Strategy as necessary throughout the Term in response to:

8.1.1 changes to applicable Laws, regulations and standards;

8.1.2 changes to Good Industry Practice;

8.1.3 any relevant Operational Changes or Contract Changes and/or associated processes;

8.1.4 any Security Incident; and

8.1.5 any reasonable request by TTL.

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

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

8.2.2 instances of misuse of the RTO System, the Services and Supplier systems used in the performance of this Agreement and access to TTL RESTRICTED, CONFIDENTIAL and SENSITIVE Data (as defined in the TTL Information Security Classification Standard listed in Schedule 2.3 (Standards)) by TTL Personnel and Supplier Personnel, including attempts at such misuse;

8.2.3 wireless access points to ensure that all wireless networks are secure and no unauthorised access points are available;

8.2.4 Malicious Software on: (i) the Supplier systems used in the delivery of the Services and, (ii) the RTO System and the Services;

8.2.5 access to and movement of TTL RESTRICTED Data, including internal access to such data; and

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

8.3 The Supplier shall ensure that access to system logs and monitoring information is strictly restricted to those Supplier Personnel who need to access these items to ensure the delivery and integrity of the RTO System and the Services.

8.4 The Supplier shall ensure that any monitoring process complies with the Monitoring Strategy and all of its legal and regulatory obligations pursuant to applicable Law.

8.5 The Supplier shall maintain a log of:

8.5.1 all instances of Supplier Personnel accessing Personal Data;

8.5.2 all TTL Personnel and Supplier Personnel logon attempts, successful and failed, to the RTO System and the Services requiring authentication;

8.5.3 all actions taken by TTL Personnel or Supplier Personnel with administrative privileges;

8.5.4 all instances of accounts being created for TTL Personnel or Supplier Personnel and their relevant privileges;

8.5.5 all records of formal staff induction by Supplier Personnel to operate systems and handle TFL RESTRICTED Data (where required);

8.5.6 all instances of accounts for TTL Personnel or Supplier Personnel being deleted;

8.5.7 Supplier Personnel system access group memberships in relation to relevant Assets;

8.5.8 group privilege changes against each of the system resources;

8.5.9 unauthorised use of input and output devices and Removable Media; and

8.5.10 all access to log files and audit systems.

8.6 The logs required under paragraph 8.5 above 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 Supplier shall implement recording mechanisms to identify TTL Personnel and Supplier Personnel 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 Supplier shall regularly review logs to identify: (i) anomalies; (ii) suspicious activity; and (iii) suspected Security Incidents. The Supplier shall notify TTL of such findings in accordance with paragraph 7.2.

8.9 The Supplier shall provide copies of any log data collected by the Supplier during its delivery of the RTO System and the Services (system audit log data) at TTL's request in a human readable electronic format such as comma-separated value or Microsoft Excel.

9. NOT USED

10. REMOVABLE MEDIA

10.1 The Supplier may only use Removable Media to support its delivery of the RTO System and the Services if it has obtained prior written consent of TTL and has implemented appropriate controls to ensure that the use of any input or output devices and Removable Media is restricted strictly to that needed to supply and support delivery of the RTO System and the Services.

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

10.3 The Supplier shall report any loss or interception of TTL Data as a result of the use of Removable Media to TTL in accordance with paragraph 7 and TTL reserves the right in such instances to rescind its approval in relation to the Supplier's continued use of Removable Media.

11. MOBILE AND HOME WORKING

11.1 The Supplier may only use mobile and home working to support its delivery of the RTO System and the Services if it has obtained prior written consent of TTL and has implemented appropriate controls to ensure continued compliance with this Schedule.

11.2 If such consent is granted but the Supplier does not have a home and mobile policy for Supplier Personnel, TTL's Home and Mobile Working Cyber Security Policy referenced in Schedule 2.3 (Standards) shall apply to the Supplier and its Supplier Personnel.

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

11.3.1 ensure through this policy that:

(a) TTL Data is protected and suitably encrypted in line with the Cyber Security Policy referenced in Schedule 2.3 (Standards), when stored outside of the Supplier Premises;

(b) TTL Data is protected when accessed, imported or exported through a connection other than one which is accessed at the Supplier Sites; and

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

11.4 The Supplier shall report any loss or interception of TTL Data as a result of home or mobile working to TTL in accordance with Clause 7.

12. DISPOSALS

12.1 The Supplier shall not reuse any Asset or Removable Media used in the delivery of the RTO Sytem and the Services unless such items have been wiped securely in accordance with a TTL agreed standard.

12.2 The Supplier shall securely dispose of and delete TTL Data from Supplier Assets used for the delivery of the RTO Sytem and the Services to a TTL agreed standard upon the termination or expiry of this Agreement or when such Supplier Assets are no longer required for the delivery of the RTO System and the Services, whichever is sooner, and documented accordingly.

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

13. SECURITY MANAGEMENT PLAN

13.1 The Outline Security Management Plan as at the Effective Date is set out at Appendix 1.

13.2 The Supplier shall, in accordance with the timescales identified within Schedule 6.1 (Transition), submit to TTL for Approval a Security Management Plan which as a minimum shall:

13.2.1 be based on the Outline Security Management Plan;

13.2.2 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the RTO System and the Services and all processes associated with the delivery of the RTO System and the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure the RTO System and the Services comply with this Schedule;

13.2.3 state any other cyber security industry standards over and above those set out in this Schedule which are applicable to the RTO System and the Services;

13.2.4 state all applicable Law which relates to the security of the RTO System and the Services; and

13.2.5 state how the Supplier shall comply with any other security requirements TTL may reasonably request from time to time.

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

13.3.1 changes to the Cyber Security Standards;

13.3.2 emerging changes in Good Industry Practice;

13.3.3 any relevant Operational Change or Contract Change and/or associated processes;

13.3.4 any new perceived or changed security threats; and

13.3.5 any reasonable request by TTL.

13.4 The Supplier shall submit any amendments to the Security Management Plan for Approval by TTL.

14. INFORMATION SECURITY MANAGEMENT SYSTEM

14.1 The Supplier shall, in accordance with the timescales set out in Schedule 6.1 (Transition), submit to TTL for Approval an ISMS, which it shall develop, implement, operate and maintain throughout the Term. The Supplier shall ensure that the ISMS includes the Security Incident Management Process, dealing with, among other matters, Security Incident management. The Supplier shall address any reasonable comments made by TTL in respect of the ISMS as soon as practicable.

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

14.2.1 the RTO System and the Services;

14.2.2 all processes associated with the delivery of the RTO System and the Services; and

14.2.3 the Sites, the Supplier Solution and any information and data (including TTL Confidential Information and TTL Data) used by TTL or the Supplier in connection with this Agreement.

14.3 The Supplier shall make any document referenced in the ISMS available to TTL 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 subject to Approval by TTL. 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 TTL.

14.5 The ISMS shall be fully reviewed in accordance with ISO/IEC 27001:2013 (which for the purpose of all references to this Standard in this Schedule shall be as updated in

accordance with Schedule 2.3 (Standards)) by the Supplier at least annually, or from time to time as agreed with TTL, in response to:

14.5.1 changes to Good Industry Practice;

14.5.2 any relevant Operational Changes or Contract Changes or proposed Operational Changes or Contract Changes and/or associated processes;

14.5.3 any new perceived or changed security threats; and

14.5.4 any reasonable request by TTL.

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

14.6.1 suggested improvements to the effectiveness of the ISMS;

14.6.2 updates to the risk assessments;

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

14.6.4 suggested improvements in measuring the effectiveness of controls.

15. COMPLIANCE WITH ISO/IEC 27001:2013

15.1 The Supplier shall obtain certification from a UKAS registered organisation of the ISMS to ISO/IEC 27001:2013 for any aspects of the business that is necessary to support the delivery of the RTO System and the Services. The Supplier shall obtain such certification in accordance with the timescales set out in Schedule 6.1 (Transition) 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 27001:2013 and Schedule 2.3 (Standards), the Supplier shall promptly notify TTL of this.

15.3 Without prejudice to any other audit rights set out in this Agreement TTL 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/IEC27001:2013.

15.4 If on the basis of evidence provided by such audits, TTL, acting reasonably, considers that compliance with the principles and practices of ISO/IEC 27001:2013 is not being achieved by the Supplier, then TTL shall notify the Supplier of the same and the Supplier shall, as soon as reasonably practicable, provide TTL 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 Supplier shall ensure that all Assets providing security enforcing functionality are certified under the CPA Scheme, to the appropriate grade, provided that relevant certified products are available in the market.

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

APPENDIX 1 – OUTLINE SECURITY MANAGEMENT PLAN

REDACTED