PENSION ADMINISTRATION SERVICES AGREEMENT

SCHEDULE 2.4

SECURITY MANAGEMENT

Version Control

VERSION	DATE	COMMENT
1.0	September 2017	Execution version

1. **DEFINITIONS**

In this Schedule, the following definitions shall apply:

"Authority Security Tests"	has the meaning given in Paragraph 8.5;
"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System and/or any information or data (including the Confidential Information and the Authority Data) used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement; and/or (c) any part of the Supplier System ceasing to be compliant with the Certification Requirements, in each case as more particularly set out in the security requirements in Schedule 2.1 (*Services Description*) and the Baseline Security Requirements;
"Certification Requirements"	the requirements set out in Paragraphs 7.1 and 7.2;
"Core Supplier System"	has the meaning given in Paragraph 4.1;
"Information Risk Management Assessment"	the assessment of the Core Supplier System in accordance with Paragraph 6 by the Authority or an independent information risk manager/professional appointed by the Authority, which results in a statement that the risks to the Core Supplier System have been appropriately considered and the residual risks reduced to an acceptable level;
"Information Risk Management Assessment Plan"	the Supplier's plan to attain a Risk Management Approval Statement from the Authority, which is prepared by the Supplier and approved by the Authority in accordance with Paragraph 6.4;
"IT Health Check"	has the meaning given Paragraph 8.1.1;
"NCSC"	the National Cyber Security Centre;
"Risk Management Approval Statement"	a notice issued by the Authority which sets out the information risks associated with using the Core Supplier System and confirms that the Authority is

	satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority;
"Risk Management Rejection Notice"	has the meaning given in Paragraph 6.7.2;
"Royal Mail Pensions Risk Management Documentation"	has the meaning given in Paragraph 6.3;
"Security Test"	has the meaning given Paragraph 8.1.4;
"Statement of Information Risk Appetite"	has the meaning given in Paragraph 5.1; and
"Vulnerability Correction Plan"	has the meaning given in Paragraph 8.2.3(a).

2. INTRODUCTION

2.1 This Schedule sets out the principles of protective security to be applied by the Supplier in performing its obligations under this Agreement and in delivering the Services.

2.2 This Schedule also sets out:

2.2.1 the process which shall apply to the Information Risk Management Assessment of the Core Supplier System;

2.2.2 the requirement for the Supplier to ensure that:

(a) the Supplier and each Sub-contractor who will Process Authority Data; and

(b) any ICT system which the Supplier or its Sub-Contractors will use to store, process or transmit Authority Data,

are and continue to be compliant with the Certification Requirements;

2.2.3 the requirements on the Supplier to conduct Security Tests; and

2.2.4 each Party's obligations in the event of an actual or attempted Breach of Security.

3. PRINCIPLES OF SECURITY

3.1 The Operations Board monitor and provide guidance to the Parties during the Information Risk Management Assessment of the Core Supplier System.

3.2 Each Party shall provide access to members of its information assurance personnel to facilitate the design, implementation, operation, management and continual improvement of the Royal Mail Pensions Risk Management Documentation and the security of the Core Supplier System and otherwise at reasonable times on reasonable notice.

4. CORE SUPPLIER SYSTEM

4.1 The information assets, ICT systems, associated business processes and/or premises which have been agreed between the Parties to constitute the core of the Supplier System are detailed in the diagrams set out in Annex 2 (together the "**Core Supplier System**").

4.2 The Parties may amend the scope of the Core Supplier System in accordance with the Change Control Procedure.

5. STATEMENT OF INFORMATION RISK APPETITE AND BASELINE SECURITY REQUIREMENTS

5.1 The Authority has provided the Supplier with its statement of information risk appetite for the Supplier System and the Services (the "**Statement of Information Risk Appetite**").

5.2 The Authority's Baseline Security Requirements in respect of the Core Supplier System are set out in Annex 1.

5.3 The Statement of Information Risk Appetite and the Baseline Security Requirements shall inform the Information Risk Management Assessment of the Core Supplier System.

6. INFORMATION RISK MANAGEMENT ASSESSMENT OF THE CORE SUPPLIER SYSTEM

6.1 The Core Supplier System shall be subject to Information Risk Management Assessment in accordance with this Paragraph 6 and reviewed annually.

6.2 The Information Risk Management Assessment shall be performed by the Authority or by representatives appointed by the Authority.

6.3 Prior to the Operational Services Commencement Date, the Supplier shall prepare and submit to the Authority the risk management documentation for the Core Supplier System, which shall comply with, and be subject to approval by the Authority in accordance with, this Paragraph 6 (the "**Royal Mail Pensions Risk Management Documentation**").

6.4 The Royal Mail Pensions Risk Management Documentation shall be structured in accordance with the template as set out in Annex 3 and include:

6.4.1 the Information Risk Management Assessment Plan, which shall include:

(a) the dates on which each subsequent iteration of the Royal Mail Pensions Risk Management Documentation will be delivered to the Authority for review and staged approval;

(b) without limiting the Authority's right to issue a Risk Management Rejection Notice pursuant to Paragraph 6.7.2:

(i) the date by which the Risk Management Approval Statement is to be issued pursuant to Paragraph 6.7.1; and

(ii) the tasks, milestones, timescales and any dependencies (including on the Authority) applicable to the issue of the Risk Management Approval Statement pursuant to Paragraph 6.7.1;

6.4.2 a risk assessment of those risks on the Risk Register which relate to the Core Supplier System and a risk treatment plan for the Core Supplier System;

6.4.3 a completed ISO 27001:2013 Statement of Applicability (SoA) for the Core Supplier System;

6.4.4 the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the

Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

6.4.5 unless otherwise specified by the Authority in writing, proposed protections that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services; and

6.4.6 evidence that the Supplier and each applicable Sub-contractor is compliant with the Certification Requirements.

6.5 If the Royal Mail Pensions Risk Management Documentation submitted to the Authority pursuant to Paragraph 6.3 (or Paragraph 6.10, as applicable) is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Royal Mail Pensions Risk Management Documentation is not approved by the Authority, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Royal Mail Pensions Risk Management Documentation following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph may be unreasonably withheld or delayed. However, any failure to approve the Royal Mail Pensions Risk Management Documentation on the grounds that it does not comply with the requirements set out in Paragraph 6.4 shall be deemed to be reasonable.

6.6 To facilitate Information Risk Management Assessment of the Core Supplier System, the Supplier shall provide the Authority and its authorised representatives with:

6.6.1 access to the Sites and the information assets within the Core Supplier System on request or in accordance with the Information Risk Management Assessment Plan; and

6.6.2 such other documentation that the Authority or its authorised representatives may reasonably require,

to enable the Authority to establish that the Core Supplier System is compliant with the Royal Mail Pensions Risk Management Documentation.

6.7 The Authority shall, by the relevant date set out in the Information Risk Management Assessment Plan, review the identified risks to the Core Supplier System and issue to the Supplier either:

6.7.1 a Risk Management Approval Statement which will then form part of the Royal Mail Pensions Risk Management Documentation, confirming that the Authority is satisfied that the identified risks to the Core Supplier System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority; or

6.7.2 a rejection notice stating that the Authority considers that the residual risks to the Core Supplier System have not been reduced to a level acceptable by the Authority and the reasons why (**"Risk Management Rejection Notice"**).

6.8 If the Authority issues a Risk Management Rejection Notice, the Supplier shall address the issues raised by the Authority in such notice within 20 Working Days (or within such other time agreed by the Authority) and shall then issue a notice to the Authority that the issues have been addressed and that the Core Supplier System is ready for a further review. The processes in Paragraph 6.7 and this Paragraph 6.8 shall be repeated following that further review until such time as the Authority issues a Risk Management Approval Statement to the Supplier, provided that if the Authority does not issue a Risk Management Approval Statement to the Supplier following the Authority's second review then the matter shall be resolved in accordance with the Dispute Resolution Procedure.

6.9 The Supplier acknowledges that it shall not be permitted to use the Core Supplier System to receive, store or Process any Authority Data prior to receiving the Risk Management Approval Statement from the Authority.

6.10 The Supplier shall keep the Core Supplier System and Royal Mail Pensions Risk Management Documentation under review and shall update the Royal Mail Pensions Risk Management Documentation annually in accordance with this Paragraph. At all times during the Term the Supplier shall maintain a register of required changes which the Supplier shall implement as part of the next annual update of the Royal Mail Pensions Risk Management Documentation. Whenever, in respect of the Core Supplier System and/or the Royal Mail Pensions Risk Management Documentation, the Supplier becomes aware (whether by way of a notification from the Authority or otherwise) that:

6.10.1 there is a significant change to the components or architecture of the Core Supplier System;

6.10.2 a new risk or vulnerability is identified to the components or architecture of the Core Supplier System;

6.10.3 there is a change in the threat profile;

6.10.4 a Sub-contractor fails to comply with the Certification Requirements;

6.10.5 there is a significant change to any risk component;

6.10.6 there is a proposal to change any of the Sites from which any part of the Services are provided;

6.10.7 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns;

the Supplier shall update the register of required changes and shall provide that updated register to the Authority on request. The Supplier shall include such updates as are contained in the register in the Royal Mail Pensions Risk Management Documentation as part of its next annual review and, following each annual review, shall submit the updated Royal Mail Pensions Risk Management Documentation to the Authority for approval as contemplated by Paragraph 6.5.

6.11 The Supplier shall review each Change Request against the Royal Mail Pensions Risk Management Documentation to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the Royal Mail Pensions Risk Management Documentation, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Authority.

6.12 The Supplier shall be solely responsible for the costs associated with developing and updating the Royal Mail Pensions Risk Management Documentation and carrying out any remedial action required by the Authority as part of the Information Risk Management Assessment process.

7. CERTIFICATION REQUIREMENTS

7.1 The Supplier shall ensure that, from the dates indicated in Clauses 7.1.1 and 7.1.2 and at all times thereafter during the Term, the Supplier and any Sub-contractor with access to Authority Data are certified as compliant with:

7.1.1 from the Effective Date, ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

7.1.2 from the relevant Milestone Date in the Implementation Plan (which shall in any event be a date prior to the Operational Services Commencement Date), Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to use the Core Supplier System to receive, store or Process any Authority Data.

7.2 The Supplier shall ensure that at all times during the Term:

7.2.1 the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data provides such service on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

7.2.2 each Sub-contractor who is responsible for the secure destruction of Authority Data is certified as compliant with the CESG Assured Service (CAS) Service Requirement Sanitisation Standard or such equivalent standard as has been approved in writing by the Authority prior to the Effective Date (and, to the extent the Supplier assumes this responsibility during the Term, the Supplier shall ensure that it has the same certification before it undertakes the relevant activities).

The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of the Authority Data.

7.3 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:

7.3.1 immediately ceases using the Authority Data; and

7.3.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with Baseline Security Requirements.

8. SECURITY TESTING

8.1 The Supplier shall, at its own cost and expense:

8.1.1 procure a CHECK IT Health Check of the Core Supplier System by an NCSC-approved member of the CHECK Scheme once every 12 months during the Term (each an "**IT Health Check**") unless additional IT Health Checks are required by Paragraph 8.2;

8.1.2 conduct vulnerability scanning and assessments of the Core Supplier System monthly;

8.1.3 conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Sub-contractors of a critical vulnerability alert from a Supplier of any software or other component of the Core Supplier System to determine whether the vulnerability affects the Core Supplier System; and

8.1.4 conduct such other tests as are required by:

(a) any Vulnerability Correction Plans;

(b) the ISO27001 certification requirements;

(c) the Royal Mail Pensions Risk Management Documentation; and

(d) the Authority following a Breach of Security or a significant change to the components or architecture of the Core Supplier System,

(each a "**Security Test**").

8.2 In relation to each IT Health Check, the Supplier shall:

8.2.1 agree with the Authority the aim and scope of the IT Health Check;

8.2.2 promptly, following receipt of each IT Health Check report, provide the Authority with a copy of the IT Health Check report;

8.2.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(a) prepare a remedial plan for approval by the Authority (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

(i) how the vulnerability will be remedied;

(ii) the date by which the vulnerability will be remedied;

(iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(b) comply with the Vulnerability Correction Plan; and

(c) conduct such further Security Tests on the Core Supplier System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

8.3 The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet any Performance Indicators, the Supplier shall be granted relief against the failure to meet such affected Performance Indicator for the period of the Security Tests.

8.4 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 8.2, the Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

8.5 Without prejudice to any other right of audit or access granted to the Authority pursuant to this Agreement, the Authority and/or its authorised representatives shall be entitled, at any time, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Core Supplier System and/or the Supplier's compliance with the Royal Mail Pensions Risk Management Documentation ("**Authority Security Tests**"). The Authority shall notify the Supplier not less than 24 hours prior to carrying out such Authority Security Test save where the Authority Security Test is required by a regulatory body or the Authority has reasonable grounds to suspect a Default by the Supplier.

8.6 The Authority shall notify the Supplier of the results of such Authority Security Tests after completion of each Authority Security Test.

8.7 The Authority Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If such Authority Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet any Performance Indicators, the Supplier shall be granted relief against the failure to meet such affected Performance Indicator to the extent directly arising as a result of the Authority and/or its authorised representatives carrying out such Authority Security Tests for the period of such Authority Security Tests.

8.8 Without prejudice to the provisions of Paragraph 8.2.3, where any Security Test carried out pursuant to this Paragraph 8 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the Core Supplier System and/or the Royal Mail Pensions Risk Management Documentation (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Supplier shall implement such changes to the Core Supplier System and/or the Royal Mail Pensions Risk Management Documentation and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible.

8.9 If the Authority unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the Royal Mail Pensions Risk Management Documentation in accordance with Paragraph 8.8 above, the Supplier shall not be deemed to be in breach of this Agreement to the extent it can be shown that such breach:

8.9.1 has arisen as a direct result of the Authority unreasonably withholding its approval to the implementation of such proposed changes; and

8.9.2 would have been avoided had the Authority given its approval to the implementation of such proposed changes.

8.10 For the avoidance of doubt, where a change to the Core Supplier System and/or the Royal Mail Pensions Risk Management Documentation is required to remedy non-compliance with the Information Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Agreement, the Supplier shall effect such change at its own cost and expense.

8.11 If any repeat Security Test carried out pursuant to Paragraph 8.8 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default.

8.12 On each anniversary of the Effective Date, the Supplier shall provide to the Authority a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:

8.12.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Agreement; and

8.12.2 the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

9. BREACH OF SECURITY – GENERAL PRINCIPLES

9.1 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other in accordance with the security incident management process as set out in the Royal Mail Pensions Risk Management Documentation.

9.2 Without prejudice to the security incident management process set out in the Royal Mail Pensions Risk Management Documentation, upon becoming aware of any of the circumstances referred to in Paragraph 9.1, the Supplier shall:

9.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority) necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Core Supplier System against any such potential or attempted Breach of Security;

(c) apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet any Performance Indicator, the Supplier shall be granted relief against the failure to meet such affected Performance Indicator for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and

(d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure;

9.2.2 as soon as reasonably practicable and, in any event, within 2 Working Days (or such longer period as is agreed by the Authority in writing), following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

9.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the Core Supplier System and/or the Royal Mail Pensions Risk Management Documentation with the Baseline Security Requirements and/or this Agreement, then such action and any required change to the Core Supplier System and/or Royal Mail Pensions Risk Management Documentation shall be completed by the Supplier at no cost to the Authority.

10. BREACH OF SECURITY – IT ENVIRONMENT

10.1 The Supplier shall, as an enduring obligation throughout the Term, use its reasonable endeavours to prevent any Breach of Security for any reason including as a result of malicious, accidental or inadvertent behaviour. This shall include an obligation to use the latest versions of anti-virus definitions, firmware and software available from industry accepted anti-virus software vendors and an obligation to comply with any Authority patching policy currently in effect and notified to the Supplier.

10.2 Notwithstanding Paragraph 10.1, if a Breach of Security is detected in the Authority System or the Supplier System, the Parties shall co-operate to reduce the effect of the Breach of Security and, particularly if the Breach of Security causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency.

10.3 All costs arising out of the actions of the Parties taken in compliance with Paragraphs 9 (excluding Paragraph 9.3) and 10.2 shall be borne by:

10.3.1 the Supplier where the Breach of Security originates from defeat of the Supplier's or any Sub-contractor's security controls, the Supplier Software, the Third Party Software or the Authority Data (whilst the Authority Data was under the control of the Supplier); or

10.3.2 the Authority if the Breach of Security originates from defeat of the Authority's security controls or Authority Data (whilst the Authority Data was under the control of the Authority),

and each Party shall bear its own costs in all other cases.

11. VULNERABILITIES AND CORRECTIVE ACTION

11.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the Core Supplier System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.

11.2 The severity of vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Royal Mail Pensions Risk Management Documentation and using the appropriate vulnerability scoring systems including:

11.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and

11.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

11.3 The Supplier shall procure the application of security patches to vulnerabilities in the Core Supplier System within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 7 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

11.3.1 the Supplier can demonstrate that a vulnerability in the Core Supplier System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Services;

11.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

11.3.3 the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Royal Mail Pensions Risk Management Documentation.

11.4 The Royal Mail Pensions Risk Management Documentation shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing.

11.5 The Supplier shall:

11.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

11.5.2 promptly notify GovCertUK of any actual or sustained attempted Breach of Security;

11.5.3 ensure that the Core Supplier System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

11.5.4 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Supplier System by actively monitoring the threat landscape during the Term;

11.5.5 pro-actively scan the Core Supplier System for vulnerable components and address discovered vulnerabilities through the processes described in the Royal Mail Pensions Risk Management Documentation;

11.5.6 from the date specified in the Information Risk Management Assessment Plan and within 5 Working Days of the end of each subsequent month during the Term, provide the Authority with a written report which details both patched and outstanding vulnerabilities in the Core Supplier System and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

11.5.7 propose interim mitigation measures to vulnerabilities in the Core Supplier System known to be exploitable where a security patch is not immediately available;

11.5.8 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Core Supplier System); and

11.5.9 inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Supplier System and provide initial indications of possible mitigations.

11.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10, the Supplier shall immediately notify the Authority.

11.7 A failure to comply with Paragraph 11.3 shall constitute a material Default.

12. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

12.1 The Supplier and Authority recognise the need for the Authority Data to be safeguarded under the Data Protection Laws. To that end, at all times the Supplier must be able to state to the Authority the physical locations within the European Economic Area where the Authority Data may be stored, processed and managed.

12.2 Save as agreed by the Authority under the Change Control Procedure as contemplated by Clause 23.3, the Supplier shall not and shall procure that the Sub-contractors do not store, process or transmit Authority Data outside the European Economic Area. The Supplier shall not make any change in location of data storage, processing and administration without the Authority's prior written agreement. Any such agreement may be subject to conditions.

12.3 The Supplier shall:

12.3.1 on demand, provide the Authority with all Authority Data in an agreed open format;

12.3.2 have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;

12.3.3 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority; and

12.3.4 securely destroy all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Agreement or, in the absence of any such requirements, in accordance with Good Industry Practice,

provided in all cases that where erasure of Authority Data or destruction of media under Paragraph 12.3.3 or 12.3.4 would contravene the requirements of a regulatory body or Law, the Supplier shall erase the Authority Data and/or destroy media (as the case may be) at the earliest date permitted under the requirements of the regulatory body or Law.

ANNEX 1

BASELINE SECURITY REQUIREMENTS

1. ROYAL MAIL PENSION DATA SECURITY PRINCIPLES

The Royal Mail Pensions Risk Management Documentation defines the security characteristics of the Services supplied under this Agreement. The Supplier shall assert, and evidence compliance, of the Services supplied under this Agreement against the data security principles contained within the Royal Mail Pensions Risk Management Documentation. The Royal Mail Pensions Risk Management Documentation describes the required security outcomes which the Services will need to achieve in order to provide the Authority with the assurance and confidence that all security risks are being appropriately managed.

2. HANDLING, PROCESSING AND STORAGE OF OFFICIAL-SENSITIVE INFORMATION

Where the Supplier is going to handle, process and store OFFICIAL-SENSITIVE information, the Supplier shall implement additional measures to secure data of this type throughout the lifecycle of the Agreement. The measures defined herein are in addition to the Supplier delivering a Service where the residual risk associated with the Service supplied under the Contract is acceptable to the Authority. The additional measures have been cross referenced to the relevant security principle headline defined within the Royal Mail Pensions Risk Management Documentation.

Serial	Security Principle Headline	Additional Measures
1.	Asset Protection and Resilience	The Supplier shall provide evidence that the infrastructure devices storing any bulk customer data shall not be directly accessible from a device hosted on the internet. In addition, the devices storing bulk data shall be located in the UK. Management and support functions may be off-shored as long as independently assured evidence can be provided that no access to user/consumer information can be obtained from off-shore locations.
2.	Governance	The Supplier shall provide evidence of robust handling processes throughout the lifecycle of all information held on the system which conforms to the definition of personal data defined within the Data Protection Act 1998 or other UK regulatory requirements. The robust handling procedures will need to specify the procedural measures implemented to ensure: • There are clearly defined roles associated with any access to bulk customer data. • Where a role is identified as having access to bulk customer data there shall be defined responsibilities which detail any actions which can be performed in support of maintaining Service availability. • There shall be a process defined which authorises Supplier staff to be able access to bulk customer data for purposes of delivering and maintaining the Service availability. • Any individual being given access to bulk customer data is aware of the HMG requirements for data protection. • The Supplier nominates an individual within its organisation who is independent from the programme delivery team and is responsible for ensuring the enforcement of the measures defined above.
3.	Operational security	This Supplier incident reporting process shall include reporting security incidents to the Data Controller and ICO

		The supplier shall agree with Authority triggers and timescales for sharing such incidents with service Enabling Authority (s) which have compromised OFFICIAL-SENISITIVE data. The Supplier shall publish and agreed with the Authority the content and format of security incident notifications for sharing information involving OFFICIAL SENISTIVE. The Supplier shall agree with the Authority a restricted distribution group with individuals who have a "need to know" for incident involving OFFICIAL SENISITIVE data.
4.	Personnel security	The Supplier shall ensure robust personal security measures for those individuals who have access OFFICAL-SENSITIVE information. Those individuals who are subject to the is more robust personnel security assurance process have the ability to access multiple User records simultaneously. This additional assurance shall provide confidence that derived from the HMG "SC" clearance or an another means which is acceptable to the Authority.

Royal Mail Pensions Data Security Principles Matrix

	Headline	Principle	Sub-points	Implementation Objectives
1	**Data in transit protection**	OFFICIAL data transiting from an Enabling Authority service consumer across untrusted networks should be adequately protected against tampering and eavesdropping (integrity and confidentiality).		Data in transit is protected between the Authority's end user devices and the service.
		OFFICIAL data transiting the Supplier's internal networks should be adequately protected against tampering and eavesdropping (integrity and confidentiality).		Data in transit is protected internally within the service.
		OFFICIAL data transiting untrusted networks should be adequately protected against tampering and eavesdropping (integrity and confidentiality).		Data in transit is protected between the service and other services (e.g. where APIs are exposed).

2	**Asset protection and resilience**	Authority data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure. OFFICIAL data shall be protected to a level which is comparable with that required under UK legislation	Physical location and legal jurisdiction	The Supplier shall ensure that the following information is made available to the Authority: The geographic locations where Authority data is stored, processed or managed from. The applicable legal jurisdictions that the Supplier operates within and how it provides comparable controls to those required under UK legislation. The Authority (where applicable) shall be informed of any changes to the above.
		OFFICIAL data shall physical protection against unauthorised access, tampering, theft and /or reconfiguration of data processing services.	Datacentre security	Data processing locations used to deliver the service are adequately protected.
		OFFICIAL data when stored on any type of removable media or storage within a service shall not be accessible by local unauthorised parties.	Data at rest protection	The Authority has confidence that removable storage media containing their data is adequately protected from unauthorised access.
		The process of provisioning, migrating and de-provisioning resources shall not result in unauthorised access to the Authority data.	Data sanitisation - retention period	The Supplier shall inform the Authority how long it will take to securely erase Authority data (including from any back-ups) from the Services.

			Data sanitisation - Authority on-boarding and off-boarding	The Supplier shall securely erase Authority data when components are moved or re-provisioned, upon request by the Authority or when the Authority leaves the service.
		Once equipment used to deliver the service reaches the end of it useful life it should be disposed of in a way that does not compromise the security of the service or Authority data	Equipment Disposal	All equipment potentially holding Authority data, credentials, or configuration information for the service shall be identified.Storage media which has held Authority data shall be appropriately sanitised or securely destroyed at the end of its lifecycle.Accounts or credentials specific to the redundant equipment are revoked.
		The service shall have the ability to operate normally in the event of failures, incidents or attacks	Physical resilience and availability	The Supplier shall clearly articulate the availability capabilities and commitments of the service. The service has adequate resiliency measures in place.
3	**Separation between tenants**	Separation should exist between Enabling Authority (s) of a service to prevent a malicious or compromised Enabling Authority from affecting the confidentiality, integrity or availability of another Enabling Authority of the service.		The Enabling Authority should be informed of any other Enabling Authority they share the platform or service with Separation between Enabling Authority (s) shall be enforced at all points within the service where the service is exposed to Enabling Authority (s). One Enabling Authority shall not be able to affect the confidentiality, integrity or availability of another Enabling Authority.

4	**Governance**	The Supplier has a security governance framework that co-ordinates and directs the provider's overall approach to the management of ICT systems, services and information.	IA Risk Management Processes	A clearly identified, and named, board representative (or a person with the direct delegated authority of) shall be responsible for the security of the cloud service. This is typically someone with the title Chief Security Officer, Chief Information Officer or Chief Technical Officer. The Supplier's security governance framework is formally documented, as are policies governing key aspects of information security relating to the service. Information security is incorporated into the Supplier's financial and operational risk reporting mechanisms for the service. The Supplier has defined roles and responsibilities for information security within the service and allocated them to named individuals. This includes a named individual with responsibility for managing the security aspects of the service. The Supplier has processes in place to identify and ensure compliance with applicable legal and regulatory requirements relating to the service.
		.	IA Organisational Maturity	The Supplier can demonstrate a sufficient degree of IA Maturity.

5	**Operational security**	The Supplier has processes and procedures in place to ensure the operational security of the service.	Configuration and change management	The status, location and configuration of service components (including hardware and software components) shall be tracked to ensure they can be effectively managed and remain securely configured. Changes to the service shall be assessed for potential security impact. They shall be managed and tracked through to completion.
			Vulnerability management	Potential new threats, vulnerabilities or exploitation techniques which could affect the service are assessed and corrective action is taken.

Protective monitoring	The service shall collect data events from all relevant Contractor devices to support effective identification that all implementation objectives are operating effectively.There shall be effective automated analysis systems in place, supported by adequately trained staff, which identify and prioritise indications in the data that may be related to malicious activities.The Supplier shall provide Authority with alerts resulting from protective monitoring which impact the implementation objectives within 24 hours. NCSC Security Operation Centre provides recommended Good Practice for the implementation of a protective monitoring solution.

-	-		Incident management	A defined process and contact route shall exist for reporting of security incidents by Enabling Authority (s) and external entities. A definition of a security incident shall be published for the service and the triggers and timescales for sharing such incidents with service Enabling Authority (s). The content and format of security incident notifications for sharing information with Enabling Authority (s) shall be published. The Supplier shall initiate investigations into incidents within five hours.
6	**Personnel security**	Supplier staff should be subjected to adequate personnel security screening and security education for their role.	Service Enabling Authority	Supplier staff that have logical or physical access to the service shall be subjected to adequate personnel security screening for their role. At a minimum these checks shall include identity, unspent criminal convictions, and right to work checks.

7	**Secure development**	Services should be designed and developed to identify and mitigate threats to their security.		The Supplier shall have a process in place to review new and evolving threats regularly and have development plans in place to progressively improve and reinforce the security of their service against these threats. Software development is carried out in line with industry good practice. Configuration management processes are in place to ensure the integrity of the components of any software. NCSC guidance on Security Design Principles for Digital Services provides best practice advice.
8	**Supply chain security**	The Supplier should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to deliver.		The Supplier shall clearly define information is shared with or accessible by its third party Contractors (and their supply chains). The Supplier's procurement processes shall ensure that the minimum relevant security requirements for all third party Contractors and delivery partners are explicitly documented. The risks to the Supplier from Sub-Contractors and delivery partners shall be regularly assessed and appropriate security controls implemented. The Supplier shall monitor its potential Sub-Contractor's compliance with security requirements and initiate remedial action where necessary.

				The Supplier's procurement process shall ensure that following contract termination all assets are returned, removed (or appropriately destroyed) and any Sub-Contractors' access rights to the Supplier's internal systems or information are removed. The Supplier shall categorise each Sub-Contractor as one of the following: Type 1 - access to aggregated Enabling Authority Consumer data Type 2 – access to limited number (less than 10) individual Enabling Authority Consumer records Type 3 – access to only part of an I individual Enabling Authority Consumer records Type 4 – no access to Enabling Authority Consumer records
9	**Secure Enabling Authority management**	The Enabling Authority should be provided with tools to enable them to securely manage their service.	Authentication of Enabling Authority to management interfaces	Only properly authorised individuals from the Enabling Authority organisation can authenticate to, and access management tools for the service. Only authorised individuals from the Enabling Authority are able to perform actions affecting the service through support channels

			Separation of Enabling Authority within management interfaces	No other Enabling Authority service consumer can access management tools for the service. The contracting shall be able to constrain permissions granted to authorised individuals from the Enabling Authority to perform actions affecting the service.
			Secure Enabling Authority Service Change Authorisation	A Supplier support procedures shall identify when a support action is security related (such as altering a user's access permissions, or changing user credentials) and ensure appropriate authorisation is in place for this change.
10	**Identity and Authentication**	Enabling Authority and Supplier access to all service interfaces should be constrained to authenticated and authorised individuals.		The Supplier shall implement controls which provide confidence that a user has authorisation to access a specific interface.
11	**External interface protection**	All external interfaces of the service should be identified and have appropriate protections to defend against attacks through them.		The service controls and protects access to elements of the service by Enabling Authority (s) and outsiders.

12	**Secure service administration**	The methods used by the Supplier's administrators to manage the operational service (monitor system health, apply patches, update configuration etc.) should be designed to mitigate any risk of exploitation which could undermine the security of the service.		The networks and devices used to perform administration /management of the service shall be appropriate to protect the Enabling Authority 's data End user devices used for administration shall be enterprise managed assets and shall be securely configured. CESG's EUD Security Guidance provides recommended good practice for configuration of a range of different end user device platforms which can be used to inform the configuration of these devices. NCSC guidance on implementation of system administration architectures provides best practice.
13	**Audit information for tenants**	Enabling Authority (s) should be provided with the audit records they need in order to monitor access to their service and the data held within it.		Audit information shall be retained for a minimum of two years or until the Enabling Authority leaves the service. The audit information shall be accessible online for a minimum of six months from the point of event collection. The Supplier shall make tenants aware of: The audit information that will be provided. The format of the data and the schedule by which it will be provisioned (e.g. on demand, daily etc).

14	**Security use of the Service by the consumer**	Service consumers are clear on their responsibilities when accessing the service.		The Service consumer understands any service configuration options available to them and the security implications The Service consumer understands the security requirements on their processes, uses and infrastructure related to use of the service. The Enabling Authority is able to educate its privileged users in how to use it safely and securely.

ANNEX 2

CORE SUPPLIER SYSTEM DIAGRAM – TECHNICAL OVERVIEW

Not Defined**<REDACTED>**

CORE SUPPLIER SYSTEM DIAGRAM – LOGICAL OVERVIEW

(1) **<REDACTED>**

ANNEX 3

ROYAL MAIL PENSIONS RISK MANAGEMENT DOCUMENTATION TEMPLATE

(1) **<REDACTED>**