**DYNAMIC FRAMEWORK**

SCHEDULE 2.4

1. Information Security And Assurance

|  |  |  |
| --- | --- | --- |
| **VERSION** | **DATE** | **COMMENT** |
| 1.0 | 10 June 2020 | Initial Release |
|  |  |  |
|  |  |  |

1. SCHEDULE 2.4
2. Information Security And Assurance
3. Introduction
   1. The scope of the Services to be provided and the quantity and type of Customer Data to be processed shall determine the level of security requirements required to be complied with by the Supplier in its performance of all Call-Off Contracts concurrently in place and being performed by the Supplier across all Customers.
   2. The level of Security Requirements applicable shall be determined based on the following criteria:
      1. the anticipated aggregate volume of data sets to be processed by the Supplier under each Call-Off Contract,
      2. the aggregate volume of Special Category Data sets to be processed by the Supplier under each Call-Off Contract,
      3. the duration of the Services; and
      4. whether or not the Supplier will have access to the Customer's systems in its delivery of the Services.

as more particularly set out in the Annex to this Schedule.

* 1. The level of security requirements shall be determined by the Supplier (and the Supplier shall notify the Customer as part of its Tender Response to a Call-Off Competition which level shall be applicable to it based on that Call-Off Contract and any already held by the Supplier) and confirmed by the Customer prior to award and shall be based on the aggregate volume of Personal Data being processed across all Call-Off Contracts the Supplier has entered into pursuant to this Framework Agreement. For clarity and by way of example, if the Supplier has 1,000 data sets (where data set means a collection of personal data which relates to an individual Service User) being processed under one Call-Off Contract (level 3 security requirements) and enters into another Call-Off Contract (for a period of less than 24 months) which related to processing of a further 2,000 data sets the aggregate total of data sets being 3,000 would mean that for both Call-Off Contracts the applicable level of security requirements would be S5. This would then also determine the corresponding level (Basic, Normal or Enhanced) under Schedule 2.3 (Standards).
  2. The Supplier shall notify each Customer of all incumbent Call-Off Contracts where and to the extent that the award of further Call-Off Contract changes the level of security requirements applicable and shall agree with the applicable Customer the timetable for implementing such changes as will be required. Each Call-Off Contract shall set out the applicable level of security requirements, as the same may be amended.
  3. In relation to the applicable level of security requirements the Supplier shall meet the corresponding security requirements as set out below.

1. principles Of Security
   1. These requirements convey the spirit and principles of the minimum information security requirements required of the Supplier, as applicable in relation to the applicable security requirements level identified in the Call-Off Order Form for a Call-Off Contract while the Supplier, its Sub-contractors, Sub-processors and supply-chain are in possession of, or maintains access to, Customer Approved Systems, information or data (including Customer Data).
   2. Due to the constant nature of evolving security threats and risks, these requirements convey principles in lieu of an exhaustive and complete description of all possible definable requirements.
   3. The Supplier shall create and maintain a proportional and holistic approach to information security in order to appropriately safeguard Customer Data including Supplier generated data or information in relation to the fulfilment of a Call-Off Contract.
   4. Due to the constant nature of evolving information risk and technical standards and guidance, a non-exhaustive list correct at the time of creation has been included within Schedule 2.3 (Standards). The Supplier is expected to review and comply with these policies, as applicable to the Security Requirements classification identified in the Call-Off Contract, throughout its provision of the Services throughout the Call-Off Term of any Call-Off Contract.
   5. The Supplier must continuously review and improve its approach to information security to ensure any associated controls or defences are appropriate, modern and proportional to adequately protect and assure data or information at any point in time.
   6. The Supplier must take all reasonable measures to ensure it (and any Sub-contractors, Sub-processors supply-chain) maintains and creates an adequate information security posture.
   7. Regardless of the security level set out below the Supplier must not Process any Customer Data outside of the UK without the prior written consent of the Customer.
   8. Regardless of the security level set out below the Supplier must inform:
      1. the Customer if there is reasonable suspicion and/or confirmation of a negative security event or Data Loss Event ("**Security Event**") that directly or indirectly processes Customer Material, Customer Confidential Information and/or Customer Data on any Customer Approved Systems and/or Supplier System relevant to the relevant Call-Off Contract within 24 hours of awareness; and
      2. inform the Authority, and all other Customers of any other Call-Off Contracts the Supplier is a Party to, that it has experienced a Security Event. Upon receipt of any such notification by the Supplier of a Security Event the Authority and any applicable Customer shall be entitled to exercise its right to audit the Supplier in accordance with Paragraph 3.6.14 to investigate the circumstances relating to any Security Event and ensure that there is no risk of a Security Event under its particular Call-Off Contract.
   9. The Supplier must provide the Customer notified in accordance with Paragraph 2.8.1 with an Incident Report following remediation to any Security Event demonstrating timescales of events from detection through to recovery.
2. Security Level Requirements
   1. Security Level 1 ("S1")
      1. The Supplier shall ensure no Customer Data is transferred electronically (by email, text, social media platform or otherwise) or otherwise contained in any systems operated or utilised by the Supplier, its Sub-contractors, Sub-processors or supply-chain in the delivery of the Services.
      2. The Customer Data, as may be necessary for the delivery of the Services or interaction with the Service User, shall be provided verbally and the Supplier shall ensure that no permanent record is made or retained of such information, by it, its Sub-contractors, Sub-processors and supply-chain members.
   2. Security Level 2 ("S2")
      1. The Supplier shall ensure that the Supplier, its Sub-contractors, Sub-processors and supply-chain of the Supplier involved in the provision of the Services:
         1. are by no later than the date immediately prior to the date on which the Supplier and any Sub-contractors, Sub-processors and supply-chain wishes to process the Customer Data, certified and compliant with Cyber Essentials Basic and shall provide a copy of such accreditation or evidence of such assurance to the Customer;
         2. all Customer Data shall be segregated and held separately from any other data held or processed by the Supplier, its Sub-contractors, Sub-processors and supply-chain;
         3. shall implement access controls to limit Supplier Personnel access to Customer Data, such that only those Supplier Personnel involved in the delivery of the Services are able to access the systems and Customer Data required for providing the Services;
         4. shall implement appropriate security measures to protect the Customer Data in accordance with Market Practice and shall prepare and submit for approval by the Customer a security controls plan ("**Information Security Management Plan**") which sets out the processes and procedures the Supplier shall have in place to ensure a good organisational approach to security under which the specific requirements of the Call-Off Contract will be met.
         5. no Customer Data (excluding Special Category Data which cannot be sent electronically unless otherwise permitted by the Customer and subject to Supplier's compliance with any such further conditions the Customer stipulates) shall be sent electronically other than by encrypted email (using a recognised encryption product or system component which reflects Market Practice);
         6. comply with the "Basic" level of Standards set out in Schedule 2.3 (Standards).
      2. Any deviation or amendment to the above shall be expressly set out in the Call-Off Contract or otherwise agreed in writing by the Customer.
      3. If the Information Security Management Plan submitted to the Customer pursuant to Paragraph 3.2.1(d) is approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Information Security Management Plan is not approved by the Customer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Customer and re-submit it to the Customer 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 fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Customer. If the Customer does not approve the Information Security Management Plan following its re-submission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Customer pursuant to this Paragraph 3.6.8 may be unreasonably withheld or delayed. However, any failure to approve the Information Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 3.2 shall be deemed to be reasonable.
      4. Approval by the Customer of the Information Security Management Plan pursuant to Paragraph 3.2.3 or of any change or amendment to the Information Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.
   3. Security Level 3 ("S3")
      1. The Supplier shall ensure that the Supplier, its Sub-contractors, Sub-processors and supply-chain of the Supplier involved in the provision of the Services:
         1. are by no later than the date immediately prior to the date on which the Supplier and any Sub-contractors, Sub-processors or supply-chain wishes to process the Customer Data, certified and compliant with any other UK Government security accreditation scheme (by way of example NHS Digital/NHS X ) and shall provide a copy of such accreditation or evidence of such assurance to the Customer;
         2. or, in the absence of such alternative accreditation:
            1. are by no later than the date immediately prior to the date on which the Supplier and any Sub-contractors, Sub-processors or supply-chain wishes to process the Customer Data, certified and compliant with Cyber Essentials Plus and shall provide a copy of such accreditation or evidence of such assurance to the Customer;
            2. all Customer Data shall be segregated and held separately from any other data held or processed by the Supplier, its Sub-contractors, Sub-processors and supply-chain;
            3. shall implement access controls to limit Supplier Personnel access to Customer Data, such that only those Supplier Personnel involved in the delivery of the Services are able to access the systems and Customer Data required for providing the Services;
            4. shall implement appropriate security measures to protect the Customer Data in accordance with Market Practice and shall prepare and submit for approval by the Customer a security controls plan ("**Information Security Management Plan**") which sets out the processes and procedures the Supplier shall have in place to ensure a good organisational approach to security under which the specific requirements of the Call-Off Contract will be met.
            5. shall provide evidence and confirmation of compliance with the Supplier's professional duties of confidentially (where applicable, for example those undertaken by medical professionals);
            6. no Customer Data (excluding Special Category Data which cannot be sent electronically unless otherwise permitted by the Customer and subject to Supplier's compliance with any such further conditions the Customer stipulates) shall be sent electronically other than by encrypted email (using a recognised encryption product or system component which reflects Market Practice);
            7. comply with the "Basic" level of Standards set out in Schedule 2.3 (Standards).
      2. Any deviation or amendment to the above shall be expressly set out in the Call-Off Contract or otherwise agreed in writing by the Customer.
      3. If the Information Security Management Plan submitted to the Customer pursuant to Paragraph 3.3.1(b)(iv) is approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Information Security Management Plan is not approved by the Customer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Customer and re-submit it to the Customer 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 fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Customer. If the Customer does not approve the Information Security Management Plan following its re-submission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Customer pursuant to this Paragraph 3.3.3 may be unreasonably withheld or delayed. However, any failure to approve the Information Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 3.3.1(b)(iv) shall be deemed to be reasonable.
      4. Approval by the Customer of the Information Security Management Plan pursuant to Paragraph 3.3.3 or of any change or amendment to the Information Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.
   4. Security Level 4 ("S4")
      1. The Supplier shall ensure that the Supplier, its Sub-contractors, Sub-processors and supply-chain of the Supplier involved in the provision of the Services:
         1. are by no later than the date immediately prior to the date on which the Supplier and any Sub-contractors, Sub-processors or supply-chain wishes to process the Customer Data, certified and compliant with any other UK Government security accreditation scheme (by way of example NHS Digital/NHS X) and shall provide a copy of such accreditation or evidence of such assurance to the Customer;
         2. or, in the absence of such alternative accreditation:
            1. are by no later than the date immediately prior to the date on which the Supplier and any Sub-contractors, Sub-processors or supply-chain wishes to process the Customer Data, certified and compliant with Cyber Essentials Plus and shall provide a copy of such accreditation or evidence of such assurance to the Customer;
            2. all Customer Data shall be segregated and held separately from any other data held or processed by the Supplier, its Sub-contractors, Sub-processors and supply-chain;
            3. implement access controls to limit Supplier Personnel access to Customer Data, such that only those Supplier Personnel involved in the delivery of the Services are able to access the systems and Customer Data required for providing the Services;
            4. implement appropriate security measures to protect the Customer Data in accordance with Market Practice and shall prepare and submit for approval by the Customer a security controls plan ("**Information Security Management Plan**") which sets out the processes and procedures the Supplier shall have in place to ensure a good organisational approach to security under which the specific requirements of the Call-Off Contract will be met.
            5. provide evidence and confirmation of compliance with the Supplier's professional duties of confidentially (where applicable, for example those undertaken by medical professionals);
            6. no Customer Data (excluding Special Category Data which cannot be sent electronically unless otherwise permitted by the Customer and subject to Supplier's compliance with any such further conditions the Customer stipulates) shall be sent electronically other than by encrypted email (using a recognised encryption product or system component which reflects Market Practice);
            7. where the delivery of the Services under the relevant Call-Off Contract involves the Supplier accessing Customer Data on a Supplier System only, the Supplier shall comply with the "Basic" level of Standards set out in Schedule 2.3 (Standards); and/or
            8. where the delivery of the Services involves the Supplier accessing Customer Data on a Supplier System and/or a Customer Approved System, the Supplier shall comply with the "Normal" level of Standards set out in Schedule 2.3 (Standards);
      2. Any deviation or amendment to the above shall be expressly set out in the Call-Off Contract or otherwise agreed in writing by the Customer.
      3. If the Information Security Management Plan submitted to the Customer pursuant to Paragraph 3.4.1(b)(iv) is approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Information Security Management Plan is not approved by the Customer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Customer and re-submit it to the Customer 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 fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Customer. If the Customer does not approve the Information Security Management Plan following its re-submission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Customer pursuant to this Paragraph 3.4.3 may be unreasonably withheld or delayed. However, any failure to approve the Information Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 3.4.1(b)(iv) shall be deemed to be reasonable.
      4. Approval by the Customer of the Information Security Management Plan pursuant to Paragraph 3.4.3 or of any change or amendment to the Information Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.
   5. Security Level 5 ("S5")
      1. The Supplier shall ensure that the Supplier, its Sub-contractors, Sub-processors and supply-chain of the Supplier involved in the provision of the Services:
         1. are by no later than the date immediately prior to the date on which the Supplier and any Sub-contractors, Sub-processors or supply-chain wishes to process the Customer Data, certified and compliant with any other UK Government security accreditation scheme (by way of example NHS Digital/NHS X) and shall provide a copy of such accreditation or evidence of such assurance to the Customer;
         2. or, in the absence of such alternative accreditation:
            1. are by no later than the date immediately prior to the date on which the Supplier and any Sub-contractors, Sub-processors or supply-chain wishes to process the Customer Data, certified and compliant with Cyber Essentials Plus and shall provide a copy of such accreditation or evidence of such assurance to the Customer; and
            2. by no later than six (6) months from the Call-Off Commencement Date, ISO/IEC 27001:2013 by a UKASS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013 or IASME Governance Standard for Information and Cyber Security by a IASME approved certification body or PAS 555:2013 by an approved certification body; and

Once the Supplier is certified in accordance with Paragraph 3.5.1(b)(ii), it shall no longer be required to maintain Cyber Essentials Plus accreditation; and

* + - * 1. by no later than six (6) months from the Call-Off Commencement Date and annually thereafter during the Call-Off Term procure a CHECK IT Health Check (ITHC) of its information systems which are involved in processing the Customer Data by a NCSC approved member of the CHECK Scheme and provide evidence of compliance with the NCSC CHECK Green Scheme,

and shall provide the Customer of each Call-Off Contract with a copy of each such certificate of compliance before the deadline for compliance as set out above.

* + - 1. where the Supplier is hosting Customer Data compliant (and able to demonstrate to compliance to the Customer's satisfaction) with the NCSC Cloud Security Principles;
      2. prepare and submit for approval by the Customer a security controls plan ("**Information Security Management Plan**") which sets out the processes and procedures the Supplier shall have in place to ensure a good organisational approach to security under which the specific requirements of the Call-Off Contract will be met.
      3. no Customer Data (excluding Special Category Data which cannot be sent electronically unless otherwise permitted by the Customer and subject to Supplier's compliance with any such further conditions the Customer stipulates) shall be sent electronically other than by encrypted email (using a recognised encryption product or system component which reflects Market Practice);
      4. comply with the "Normal" level of Standards set out in Schedule 2.3 (Standards).
    1. Any deviation or amendment to the above shall be expressly set out in the Call-Off Contract or agreed in writing by the Customer.
    2. If the Information Security Management Plan submitted to the Customer pursuant to Paragraph 3.5.1(d) is approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Information Security Management Plan is not approved by the Customer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Customer and re-submit it to the Customer 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 fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Customer. If the Customer does not approve the Information Security Management Plan following its re-submission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Customer pursuant to this Paragraph 3.5.3 may be unreasonably withheld or delayed. However, any failure to approve the Information Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 3.5.1(d) shall be deemed to be reasonable.
    3. Approval by the Customer of the Information Security Management Plan pursuant to Paragraph 3.5.3 or of any change or amendment to the Information Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.
  1. Security Level 6 ("S6")

**Certification Requirements**

* + 1. The Supplier shall ensure that the Supplier, its Sub-contractors, Sub-processors and supply-chain of the Supplier involved in the provision of the Services are:
       1. by no later than the date immediately prior to the date on which the Supplier and any Sub-contractors, Sub-processors or supply-chain wishes to process the Customer Data, certified and compliant with any other UK Government security accreditation scheme (by way of example NHS Digital/NHS X) and shall provide a copy of such accreditation or evidence of such assurance to the Customer;
       2. or, in the absence of such alternative accreditation:
          1. are by no later than the date immediately prior to the date on which the Supplier and any Sub-contractors, Sub-processors or supply-chain wishes to process the Customer Data, certified and compliant with Cyber Essentials Plus and shall provide a copy of such accreditation or evidence of such assurance to the Customer; and
          2. by no later than six (6) months from the Call-Off Commencement 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 or IASME Governance Standard for Information and Cyber Security by a IASME approved certification body or PAS 555:2013 by an approved certification body; and

Once the Supplier is certified in accordance with Paragraph 3.6.1(b)(ii), it shall no longer be required to maintain Cyber Essentials Plus accreditation; and

* + - * 1. by no later than six (6) months from the Call-Off Commencement Date and annually thereafter during the Call-Off Term procure a CHECK IT Health Check (ITHC) of its information systems which are involved in processing the Customer Data by a CESG approved member of the CHECK Scheme and provide evidence of compliance with the NCSC CHECK Green Scheme,

and shall provide the Customer of each Call-Off Contract with a copy of each such certificate of compliance before the deadline for compliance as set out above.

* + 1. Without limiting Paragraphs 3.6.1(a) or 3.6.1(b) (as applicable) the Supplier acknowledges that it is responsible for ensuring security of the Customer Data, and all derivatives of the Customer Data created, used and Processed by the Supplier, its Sub-contractors, Sub-processors and/or supply-chain of the Supplier in the performance of the Services and the Supplier shall ensure at all times during the Call-Off Term that all such Sub-contractors, Sub-processors and supply-chain of the Supplier with access to Customer Data or who will Process Customer Data have appropriate security in place to protect the applicable Customer Data as applicable and shall ensure that:
       1. each Sub-contractor, Sub-processor and member of its supply chain has an appropriate security governance structure in place to support the Supplier to meet its obligations as set out below in relation to the Information Security Management Plan, information risk assessment, oversight and auditing; and
       2. the Supplier shall have in place an appropriate written contract with each Sub-contractor Sub-processor or member of its supply chain that ensures appropriate security measures are in place, which manages risk and responsibility and that the Supplier has undertaken appropriate information assurance in relation to such Sub-contractors, Sub-processor or member of its supply chain to ensure that all such security controls are effective.

Any exceptions to the flow-down of requirements to Sub-contractors, Sub-processor or, member of its supply chain must be agreed with the Customer.

* + 1. The Supplier shall notify each Customer that it has a Call-Off Contract with at the relevant time and the Customer as soon as reasonably practicable and, in any event within two (2) Working Days, if the Supplier, Sub-processor or member of its supply chain ceases to be compliant with the certification requirements set out above in Paragraphs 3.6.1(a) or 3.6.1(b) (as applicable) and on request from any one or more Customer, shall or shall procure that the relevant Sub-contractor, Sub-processor or member of its supply chain shall:
       1. immediately cease using the Customer Data of the requesting Customer; and
       2. procure that the Supplier, its Sub-contractors, Sub-processors or member of its supply chain promptly returns, destroys and/or erases the Customer Data of the relevant requesting Customer in accordance with Baseline Security Requirements.

**Governance**

* + 1. The Supplier shall create as required prior to the processing of Customer Data, and thereafter maintain, an adequate and robust information security governance regime.
    2. No later than six (6) weeks prior to any Call-Off Commencement Date, the Supplier shall prepare and submit to the Customer for approval in accordance with Paragraph 3.6.8 a fully developed, complete and up-to-date plan for the management of information security ("**Information Security Management Plan**") which shall comply with the requirements of Paragraph 3.6.7 and ‎ISO/IEC 27001 or such alterative security accreditation confirmed in Paragraphs 3.6.1. If the Supplier has not achieved its ISO27001 certification or such alterative security accreditation confirmed in Paragraphs 3.6.1 by this point, the Information Security Management Plan shall be prepared on the basis of the requirements of ISO/IEC 27001 or such alterative security accreditation confirmed in Paragraphs 3.6.1 and any changes required to be made to the Information Security Management Plan as a consequence of future ISO/IEC certification /alternative accreditation shall be agreed between the Supplier and the Customer by way of the Change Control Procedure by no later than the date six (6) months from the Call-Off Commencement Date.
    3. The Parties acknowledge that the purpose of the Information Security Management Plan is to ensure a good organisational approach to security under which the specific requirements of the Call-Off Contract will be met.
    4. The Information Security Management Plan shall:
       1. comply with ‎ISO/IEC 27001 or such alterative security accreditation confirmed in Paragraphs 3.6.1;
       2. identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
       3. detail the process for managing any security risks from Sub-contractors, Sub-processor or member of its supply chain and third parties authorised by the Customer with access to the Services, processes associated with the delivery of the Services, the Customer Premises, the Sites, the Supplier Systems, the Customer Approved Systems (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Customer Materials, Customer Confidential Information and the Customer Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;
       4. unless otherwise specified by the Customer in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Customer Premises, the Sites, the Supplier System, the Customer Approved System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Customer Materials, Confidential Information and the Customer Data) to the extent used by the Customer or the Supplier in connection with the Call-Off Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;
       5. set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule;
       6. be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002 or such alterative security accreditation confirmed in Paragraphs 3.6.1, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and
       7. be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Customer engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.
    5. If the Information Security Management Plan submitted to the Customer pursuant to Paragraph 3.6.5 is approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Information Security Management Plan is not approved by the Customer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Customer and re-submit it to the Customer 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 fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Customer. If the Customer does not approve the Information Security Management Plan following its re-submission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Customer pursuant to this Paragraph 3.6.8 may be unreasonably withheld or delayed. However, any failure to approve the Information Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 3.6.7 shall be deemed to be reasonable.
    6. Approval by the Customer of the Information Security Management Plan pursuant to Paragraph 3.6.8 or of any change or amendment to the Information Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.
    7. The Information Security Management Plan and ISO/IEC 27001 certification or such alterative security accreditation confirmed in Paragraphs 3.6.1 must have an adequate scope to encompass all possible methods, locations and Supplier Personnel that may be utilised in the processing of Customer Data.
    8. The Information Security Management Plan scope must include applicable policies such as malware policies, software patching policies and password standards.
    9. The Information Security Management Plan and ISO/IEC 27001 certification or such alterative security accreditation confirmed in Paragraphs 3.6.1 must be evidenced to the Customer on demand, including but not limited to, statements of scope and applicability, risk management plans and documentation and any other related artefacts.
    10. The Supplier shall, where a specific person is named as such in Schedule 9.2 (Call-Off Key Personnel) of a Call-Off Contract, appoint a security and information risk manager who shall be the person accountable for the Supplier's information risk and security management.
    11. The Customer retains rights to audit (in accordance with the provisions of the relevant Call-Off Contract) the Supplier's information security posture at any time and the Supplier will provide relevant certifications, information, data and artefacts applicable to the same on demand, including but not limited to, physical access for the purposes of audit to locations used to process Customer Data subject to scheduling and adequate notice periods being provided by the Customer to the Supplier.
    12. Security must be embedded by the Supplier in all service management, including but not limited to, change management, incident management, and other service management artefacts as described within ISO/IEC 20000 (and any equivalent replacement certification or such alterative security accreditation confirmed in Paragraphs 3.6.1).
    13. The Supplier's organisation, including but not limited to, the Supplier Systems and Supplier Personnel used or involved in the fulfilment of the Call-Off Contract, must adhere to all applicable Laws or regulation, including but not limited to Data Protection Legislation and comply with the relevant provisions of the Call-Off Contract.
    14. The Supplier Information Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
        1. emerging changes in Market Practice;
        2. any change or proposed change to the IT Environment, the Services and/or associated processes;
        3. any new perceived or changed security threats;
        4. any changes to its Sub-contractors or any changes made by its Sub-contractors; and
        5. any reasonable change in requirement requested by the Customer.
    15. The Supplier shall provide the Customer with the results of such reviews as soon as reasonably practicable after their completion and amend the Information Security Management Plan at no additional cost to the Customer.
    16. Subject to Paragraph 3.6.20, any change which the Supplier proposes to make to the Information Security Management Plan (as a result of a review carried out pursuant to Paragraph 3.6.17, on Customer request or otherwise) shall, save as set out in this Paragraph, be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Customer:
        1. any operational change made by the Supplier, Sub-contractors, Sub-processor, member of its supply chain which does not impact the Customer's Approved Systems or changes the output of the delivery of the Services shall be notified to the Customer by the Supplier as part of the annual review but does not require approval from the Customer;
        2. any change made to provide immediate mitigation to a security breach or to ensure and protect the security of the Customer Data and any Supplier generated data or information in relation to the fulfilment of the Call-Off Contract.
    17. The Customer may, where it is reasonable to do so, approve and require changes or amendments to the Information Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of the Call-Off Contract.

**Assurance**

* + 1. The Supplier shall (and shall ensure that its Sub-contractors, Sub-processor or member of its supply chain shall) perform its obligations in accordance with the obligations set out in this Schedule and in accordance with the "Enhanced" level of Standards set out in Schedule 2.3 (Standards). The Supplier may not utilise Customer Data or Customer Approved Systems for purposes other than those permitted by the Call-Off Contract and take all proportional measures to ensure the same.

**Access, Authorisation, Authentication and Audit**

* + 1. The Supplier Systems, including those controlling access to physical locations, must have auditable authorisation, authentication and access control based on least privilege, and aligned appropriately to the business and individual user requirements.
    2. The Supplier Systems must ensure logical separation between purposes and zones of trust, for example, logical delineation between Supplier Systems involved in the delivery of the Services and development environments used to iterate and improve the Supplier Systems involved in the delivery of the Services. Such separation must include, but not be limited to, the unique credentials and the prohibition of the use of Customer Data for non-service fulfilment (for example, testing) purposes unless authorised in advance by the Customer in writing.
    3. The Supplier's access to the Customer Approved Systems must be limited to only systems, services and Supplier Personnel directly required for the performance of the Services in accordance with the terms of the Call-Off Contract. The Supplier shall notify the Customer in advance of the proposed Supplier Personnel who require access to the Customer Approved Systems. No Supplier Personnel shall be permitted to access the Customer Approved Systems until the Customer has provided its approval of each individual in advance, any approval is subject to identification verification and security assurance checks undertaken by the Customer.

**Risk Assessment & Management**

* + 1. The Supplier must undertake informational risk assessment(s) of any component, including but not limited to systems, services, personnel, physical locations and supply chain (including all Sub-contractors, Sub-processor or member of its supply chain), utilised or otherwise involved in the provision of the Services.
    2. Holistic informational risk assessment(s) must support the Supplier's Information Security Management Plan and proactively recommend additional controls to be proportionally implemented to continuously iterate and improve the Supplier's information security regime.
    3. The Supplier must disclose informational risk assessment information on request to the Customer.

**Awareness & Training**

* + 1. Supplier Personnel must be provided with adequate and relevant security-related education, training and awareness and include, but not be limited to, technical, physical and procedural security.
    2. Education, training and awareness courses or certifications must be completed by all Supplier Personnel utilised in the direct or indirect performance of the Services at once (x1) in every Call-Off Contract Year.

**Personnel Security**

* + 1. Save where otherwise agreed in writing by the Customer, the Supplier warrants that all Supplier Personnel are assured to the UK Government Baseline Personnel Security Standard prior to the ability to directly, or indirectly, access or influence Customer Approved Systems or Customer Data. For clarity any agreement by the Customer that any Supplier Personnel are not required to meet such assurance level is solely where their access to the Customer Data is minimal, does not contain special category data or the Supplier is able to provide an equivalent level of assurance appropriate to the Customer Data which will be Processed by any such Sub-contractor personnel.
    2. Additional Supplier Personnel clearances or vetting may be required and will be determined and notified by the Customer on a case-by-case basis from time to time.
    3. The cost of additional Supplier Personnel clearances or vetting is the responsibility of the Supplier while the sponsorship for the same is the responsibility of the Customer.

**Technical Security**

* + 1. The Supplier warrants that all Supplier Systems operated by the Supplier or Customer Approved Systems utilised directly by the Supplier, in the performance of the Services are configured and maintained in accordance with corresponding vendor best practices or as superseded by Market Practice, including but not limited to vulnerability and patch management through an aggressive patching regime and security-related change control to avoid regression or introduction of a negative security benefit.
    2. The Supplier must continuously review technical security measures to ensure any appropriate, applicable and proportional changes are applied in response to change in accordance with changes to government and industry guidance.
    3. Supplier technical security standards, policies and guidance should align to UK National Cyber Security Centre (NCSC) publications and guidance wherever suitable. The Customer reserves the right to request information on, and audit, the same.
    4. The Supplier must ensure technical solutions and services adopt modern connectivity and cryptographic standards once applicable guidance and standards have been updated, including but not limited to, implementing iterations to in-transit encryption such as Transport Layer Security (TLS) and Internet Protocol Security (IPSec) and at-rest encryption.

**Operational Security & Incident Management**

* + 1. The Supplier must create and maintain a robust operational security posture to ensure the proactive defences from threats to Customer Data including but not limited to, awareness, detection, prevention, response and remediation processes/controls to effectively manage and remediate information security related events or incidents.
    2. The Supplier must conduct continuous vulnerability, security, penetration testing and produce security improvement plans to address any issues raised by the same.
    3. Information security related monitoring must be carried out by the Supplier in line with modern best practices and as required by risk assessment and the Supplier's Information Security Management Plan.
    4. The Supplier must create and maintain adequate forensic readiness capability to facilitate independent review(s) of information security events or incidents. Such readiness must include, but not be limited to, granular access control data, technical network traffic data and a detailed timeline of events per event or incident.
    5. Security incidents shall be managed in accordance with Paragraphs 2.8 and 2.9.

**Business Continuity**

* + 1. In addition to the Supplier's obligations under Schedule 8.6 (Service Continuity Plan and Corporate Resolution Planning) where applicable, the Supplier shall appropriately backup and/or archive Customer Data and any data arising from the Services at least once (x1) every 24 hours.
    2. The Supplier shall ensure that any data backup or archiving locations meet the information security requirements of the original data source.
    3. The Supplier shall no less than Quarterly test and assure any backup and archival systems are functional, including but not limited to, a functional data restoration test to validate that restoration functional of the backup and archival systems are functional as designed and required by the Supplier's business continuity policies and plans.

**Audit and Protection Monitoring**

* + 1. The Supplier shall collect audit records which relate to security events in delivery of the Services or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness. Such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Customer Data. The retention periods for audit records and event logs must be agreed with the Customer and documented.

**Annex**

**SECURITY MATRIX**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Volume of Data (no. of data subjects) | Volume of Special Category Data (no. of data subjects) | Value of Services | Duration of Services | Access to MoJ Systems |
| S1  Beneficiaries eg Individuals and small localised charities etc, receiving Service User assistance | <10 | 0 | <£30k | <12 months | No |
| S2  Examples:  Local or independent charities  Parish Councils  Local Public Service Provider | <100 | 0 | <£50k | <12 months | No |
| S3  Examples:  Health, social care and well being, which includes 3rd Party health provision and mental health support  Local Councils | <1000 | Recipient is a registered medical practitioner or other professional subject to a professional duty of confidentiality | £100k | <12 months | No |
| S4  Examples:  Local Councils  National Charity | <1000 | Any | <£100k | <12 months | See options in security requirements |
| S5  Examples:  BASS (NACRO)  National Charity | <2500 | Any | <250k | <24 months | Yes |
| S6  Examples:  CRC | >2500 | Any | Any | Any | Yes |