Call Off Schedule 7 Security

1. Definitions
   1. In this Call Off Schedule 7, the following definitions shall apply:

|  |  |
| --- | --- |
| **"Accreditation"** | the assessment of the Core Information Management System in accordance with Paragraph 6 by the Customer or an independent information risk manager/professional appointed by the Customer, which results in an Accreditation Decision; |
| **"Accreditation Decision"** | is the decision of the Customer, taken in accordance with the process set out in Paragraph 6, to issue the Supplier with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System; |
| **"Accreditation Plan"** | the Supplier's plan to attain a Risk Management Approval Statement from the Customer, which is prepared by the Supplier and approved by the Customer in accordance with Paragraph 6.6; |
| **“Anti-Malicious Software”** | means software that scans for and identifies possible Malicious Software in the ICT Environment; |
| **“Asset Owner”** | has the meaning given in paragraph 4 (Definitions) of Call Off Schedule 2 (Services) |
| **“Asset Owner Data”** | data from Asset Owners provided directly to the Supplier, by Asset Owners, in accordance with the terms of the Data Distribution Agreements for the purposes of the development and operation of the NUAR; |
| **“Baseline Security Requirements”** | means those requirements set out in Annex 1. |
| **"Breach of Security"** | the occurrence of:   1. any unauthorised access to or use of the Services, the Customer Premises, the Sites, the Supplier System, the Customer System and/or any information or data (including the Confidential Information and the Customer Platform Data) used by the Customer, the Supplier or any Sub-Contractor in connection with this Call Off Contract; 2. the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Customer Platform Data), including copies of such information or data, used by the Customer, the Supplier or any Sub- Contractor in connection with this Call Off Contract; and/or 3. 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 Framework Schedule 2 (Specification) and the Call Off Order Form and the Baseline Security Requirements; |
| **“Customer Platform Data”** | Customer Data and Asset Owner Data; |
| **"Customer System"** | the Customer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Customer or the Supplier in connection with this Call Off Contract which is owned by or licensed to the Customer by a third party and which interfaces with the Supplier System or which is necessary for the Customer to receive the Deliverables; |
| **"Certification Requirements"** | the requirements set out in Paragraphs 7.1 to 7.6, inclusive; |
| **“CHECK Service Provider”** | means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the IT Health Check services required by Paragraph 8.1.1 ; |
| **“CIMS Sub-Contractor”** | a Sub-Contractor that provides or operates the whole, or a substantial part, of the Core Information Management System; |
| **“Commercial off the shelf Software” or “COTS Software”** | Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms; |
| **"Core Information Management System" or “CIMS”** | those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-Contractors to Process Customer Platform Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources) which the Customer has determined in accordance with Paragraph 4.2 shall be subject to Accreditation; |
| **“Data Distribution Agreement”** | the meaning given in paragraph 4 (Definitions) of Call Off Schedule 2 (Services) |
|  |  |
| **“Higher Risk Sub-Contractor”** | means a Sub-Contractor that Processes Customer Platform Data, where that data includes:   1. data classified at OFFICIAL-SENSITIVE or above |
| **"ICT Environment"** | the Customer System and the Supplier System; |
| **"Information Management System"** | means the Core Information Management System and the Wider Information Management System; |
| **"IT Health Check"** | has the meaning given Paragraph 8.1.1; |
| **"Malicious Software"** | any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence; |
| **“Medium Risk Sub-Contractor"** | means a Sub-Contractor that Processes Customer Platform Data, where that data includes:   1. data classified as OFFICIAL-SENSITIVE |
| **“NCSC”** | means the National Cyber Security Centre; |
| **“NUAR”** | has the meaning given in paragraph 4 (Definitions) of Call Off Schedule 2 (Services); |
| **“Personal Data Breach”** | has the meaning given in the Data Protection Legislation; |
| **“Personal Data Processing Statement”** | sets out: (i) the types of Personal Data which the Supplier and/or its Sub-Contractors are Processing on behalf of the Customer; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-Contractors are Processing on behalf of the Customer; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Sub-Contractors Process Customer Platform Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Sub-Contractors have implemented to protect the Customer Data against a Breach of Security including a Personal Data Breach, which shall be prepared by the Supplier in accordance with Paragraph 6.4 and included in the risk management documentation; |
| **"Process Customer Platform Data"** | any operation which is performed on Customer Platform Data, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, organising, publishing retrieving, storing, structuring, transmitting or otherwise using Customer Platform Data; |
| **"Required Changes Register"** | is a register which forms part of the Security Management Plan which records each of the changes that the Supplier has agreed with the Customer shall be made to the Core Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 6.14.1 together with the date on which each such change shall be implemented and the date on which each such change was implemented; |
| **"Risk Management Approval Statement"** | a notice issued by the Buyer which sets out the information risks associated with using the Core Information Management System and confirms that the Buyer is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer; |
| **"Risk Management Reject Notice"** | has the meaning given in Paragraph 6.8.2; |
| **"Security Management Plan"** | has the meaning given in Paragraph 6.5; |
| **"Security Test"** | has the meaning given Paragraph 8.1; and |
| **“Special Category Personal Data”** | means the categories of Personal Data set out in article 9(1) of the GDPR. |
| **"Statement of Information Risk Appetite"** | has the meaning given in Paragraph 5.1;. |
| **“Sub-Contractor Security Requirements”** | means those requirements set out in Annex 2. |
| **"Supplier System"** | the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Customer System); |
| **"Vulnerability Correction Plan"** | has the meaning given in Paragraph 8.3.3(a); and |
| **"Wider Information Management System"** | those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-Contractors to Process Customer Platform Data which have not been determined by the Customer to form part of the Core Information Management System, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources). |

1. Introduction
   1. This Call Off Schedule sets out:
      1. the arrangements the Supplier must implement before, and comply with when, providing the Services, (or if expressly permitted by the Authority, before Processing Customer Platform Data), performing its other obligations under this Call Off Contract to ensure the security of the Customer Platform Data, the ICT Environment, the Services and the Information Management System;
      2. the process which shall apply to the Accreditation of the Core Information Management System in Paragraph 6;
      3. the Certification Requirements applicable to the Wider Information Management System in Paragraph 7;
      4. the Security Tests which the Supplier shall conduct during the Call Off Contract Period in Paragraph 8;
      5. the Security Tests which the Customer may conduct during the Call Off Contract Period in Paragraph 8.6;
      6. the requirements to patch vulnerabilities in the Core Information Management System in Paragraph 9;
      7. the obligations on the Supplier to prevent the introduction of Malicious Software into the Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Information Management System in Paragraph 11; and
      8. each Party's obligations in the event of an actual or attempted Breach of Security in Paragraph 11.
2. Principles of Security
   1. The Supplier acknowledges that the Customer places great emphasis on the confidentiality, integrity and availability of the Customer Platform Data and, consequently on the security of:
      1. the Sites;
      2. the ICT Environment;
      3. the Services; and
      4. the Core Information Management System.
   2. Notwithstanding the involvement of the Customer in the Accreditation of the Core Information Management System, the Supplier shall be and shall remain responsible for:
      1. the security, confidentiality, integrity and availability of the Customer Platform Data whilst that Customer Platform Data is under the control of the Supplier or any of its Sub-Contractors; and
      2. the security of the Information Management System.
   3. The Supplier shall:
      1. comply with the Baseline Security Requirements; and
      2. ensure that each Sub-Contractor that Processes Customer Platform Data complies with the Sub-Contractor Security Requirements.
   4. The NUAR Programme Board shall, in addition to its responsibilities set out that Schedule, monitor and may also provide recommendations to the Supplier on the Accreditation of the Core Information Management System.
   5. To facilitate the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Information Management System and otherwise:
      1. the Supplier shall provide access to the Supplier Personnel responsible for information assurance; and
      2. the Customer shall provide access to its personnel responsible for information assurance at reasonable times on reasonable notice.
3. Information Management System
   1. The Information Management System comprises the Core Information Management System and the Wider Information Management System.
   2. The Customer shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Customer to make such determination, the Supplier shall provide the Customer with such documentation and information that the Customer may reasonably require regarding any information assets, ICT systems and/or Sites which will be used by the Supplier or any Sub-Contractor to Process Customer Platform Data together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources). The Customer shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System. The Supplier shall reproduce the Customer’s decision as a diagram documenting the Core Information Management System, the Wider Information Management system and the boundary between the two. This diagram shall form part of the Security Management Plan.
   3. Any proposed change to the component parts of the Core Information Management System or the boundary between the Core Information Management System and the Wider Information Management System shall be notified and processed in accordance with Clause 23 of this Call Off Contract (Change) .
4. Statement of Information Risk Appetite and Baseline Security Requirements
   1. The Supplier acknowledges that the Customer has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services (the "**Statement of Information Risk Appetite**").
   2. The Customer's Baseline Security Requirements in respect of the Core Information Management System are set out in Annex 1.
5. Accreditation of the Core Information Management System
   1. The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 6.
   2. The Supplier acknowledges that the purpose of Accreditation is to ensure that:
      1. the Security Management Plan accurately represents the Core Information Management System;
      2. the Accreditation Plan, if followed, provides the Customer with sufficient confidence that the CIMS will meet the requirements of the Baseline Security Requirements and the Statement of Risk Appetite; and
      3. the residual risks of the Core Information Management System are no greater than those provided for in the Statement of Risk Appetite and Baseline Security Requirements.
   3. The Accreditation shall be performed by the Customer or by representatives appointed by the Customer.
   4. In addition to any obligations imposed by Call Off Schedule 4 (Project Plan) the Supplier must ensure that its Project Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call Off Schedule 7 (Security), including any requirements imposed on Sub-Contractors by Annex 1, from the Call Off Commencement Date.
   5. By the date specified in the Project Plan, the Supplier shall prepare and submit to the Customer the risk management documentation for the Core Information Management System, which shall be subject to approval by the Customer in accordance with, this Paragraph 6 (the "**Security Management Plan**").
   6. The Security Management Plan shall be structured in accordance with the template as set out in Annex 3 and include:
      1. the Accreditation Plan, which shall include:
         1. the dates on which each subsequent iteration of the Security Management Plan will be delivered to the Customer for review and staged approval; and
         2. the date by which the Supplier is required to have received a Risk Management Approval Statement from the Customer together with details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Customer responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 6.8.1.
      2. a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;
      3. a completed ISO 27001:2013 Statement of Applicability for the Core Information Management System;
      4. the process for managing any security risks from Sub-Contractors 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 System, the Customer System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Confidential Information of the Customer and the Customer Platform Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;
      5. unless such requirement is waived by the Customer, proposed controls that will be implemented in respect of 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 System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Confidential Information of the Customer and the Government Data) to the extent used by the Customer or the Supplier in connection with this 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;
      6. the Required Changes Register;
      7. evidence that the Supplier and each applicable Sub-Contractor is compliant with the Certification Requirements;
      8. a Personal Data Processing Statement; and
      9. the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between the two created under Paragraph 4.2.
   7. To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Customer and its authorised representatives with:
      1. access to the Sites, ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Accreditation Plan; and
      2. such other information and/or documentation that the Customer or its authorised representatives may reasonably require, to enable the Customer to establish that the Core Information Management System is compliant with the Security Management Plan.
   8. The Customer shall, by the relevant date set out in the Accreditation Plan, review Security Management Plan and issue to the Supplier either:
      1. a Risk Management Approval Statement which will then form part of the Security Management Plan, confirming that the Customer is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Customer; or
      2. a rejection notice stating that the Customer considers that the identified risks to the Core Information Management System have not been adequately or appropriately addressed or the residual risks to the Core Information Management System have not been reduced to the level anticipated by the Statement of Information Risk Appetite, and the reasons why (**"Risk Management Rejection Notice"**).
   9. If the Customer issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:
      1. address all of the issues raised by the Customer in such notice;
      2. update the Security Management Plan, as appropriate, and
      3. notify the Customer that the Core Information Management System is ready for an Accreditation Decision.
   10. If the Customer issues a two or more Risk Management Rejection Notices, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Customer may by terminate this Call Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 42.2 of this Call Off Contract  .
   11. Subject to Paragraph 6.10, the process set out in Paragraphs 6.8 to 6.10 shall be repeated until such time as the Customer issues a Risk Management Approval Statement to the Supplier or terminates this Call Off Contract.
   12. The Supplier shall not use the Core Information Management System to Process Customer Platform Data prior to receiving a Risk Management Approval Statement.
   13. The Supplier shall keep the Core Information Management System and Security Management Plan under review and shall update the Security Management Plan annually in accordance with this Paragraph and the Customer shall review the Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 6.15.
   14. The Supplier shall notify the Customer within 2 Working Days after becoming aware of:
       1. a significant change to the components or architecture of the Core Information Management System;
       2. a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;
       3. a change in the threat profile;
       4. a Sub-Contractor failure to comply with the Core Information Management System code of connection;
       5. a significant change to any risk component;
       6. a significant change in the quantity of Personal Data held within the Core Information Management System;
       7. where the Supplier has previously Processed Personal Data that does not include Special Category Personal Data, it starts to Process Special Category Personal Data, other than data relating to accessibility or dietary requirements relating to an individual;
       8. a proposal to change any of the Sites from which any part of the Services are provided; and/or
       9. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns; and
       10. the Supplier shall update the Required Changes Register and provide the updated Required Changes Register to the Customer for review and approval within 10 Working Days after the initial notification or such other timescale as may be agreed with the Customer.
   15. If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Customer, such failure shall constitute a material Default and the Supplier shall:
       1. immediately cease using the Core Information Management System to Process Customer Platform Data until the Default is remedied, unless directed otherwise by the Customer in writing and then it may only continue to Process Customer Platform Data in accordance with the Customer's written directions; and
       2. where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Customer and, should the Supplier fail to remedy the Default within such timescales, the Customer may terminate this Call Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 42.2 of this Call Off Contract
   16. The Supplier shall review any request for Variation (under Clause 23 of this Call-Off Contract) against the Security Management Plan to establish whether the documentation would need to be amended should such Variation be agreed and, where a Variation would require an amendment to the Security Management Plan, 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 Customer.
   17. The Supplier shall be solely responsible for the costs associated with developing and updating the Security Management Plan and carrying out any remedial action required by the Customer as part of the Accreditation process.
6. Certification Requirements
   1. The Supplier shall ensure, at all times during the Call Off Contract Period, that it is certified as compliant with:
      1. 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
      2. Cyber Essentials PLUS, and shall provide the Customer 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 Information Management System to receive, store or Process any Customer Platform Data.
   2. Notwithstanding anything else in this Contract, a CIMS Sub-Contractor shall be treated for all purposes as a Key Sub-Contractor.
   3. In addition to the obligations contained in Clause 30.2 of this Call Off Contract, the Supplier must ensure that the Key Sub-Contract with each CIMS Sub-Contractor:
      1. contains obligations no less onerous on the Key Sub-Contractor than those imposed on the Supplier under this Call Off Schedule 7 (Security); but
      2. provides for the Customer to perform Accreditation of any part of the Core Information Management System that the CIMS Sub-Contractor provides or operates which is not otherwise subject to Accreditation under this Call Off Schedule 7 (Security).
   4. The Supplier shall ensure that each Higher Risk Sub-Contractor is certified as compliant with either:
      1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or
      2. Cyber Essentials PLUS,

and shall provide the Customer with a copy of each such certificate of compliance before the Higher-Risk Sub-Contractor shall be permitted to receive, store or Process Customer Platform Data.

* 1. The Supplier shall ensure that each Medium Risk Sub-Contractor is certified compliant with Cyber Essentials.
  2. The Supplier shall ensure that the Supplier and each Sub-Contractor who is responsible for the secure destruction of Customer Platform Data:
     1. securely destroys Customer Platform Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and
     2. are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Customer.
  3. The Supplier shall provide the Customer 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 Customer Platform Data.
  4. The Supplier shall notify the Customer 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 Customer, shall or shall procure that the relevant Sub-Contractor shall:
     1. immediately ceases using the Customer Platform Data; and
     2. procure that the relevant Sub-Contractor promptly returns, destroys and/or erases the Customer Platform Data in accordance with Baseline Security Requirements.
  5. The Customer may agree to exempt in whole or part the Supplier or any Sub-Contractor from the Certification Requirements. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

1. Security Testing
   1. The Supplier shall, at its own cost and expense:
      1. procure testing of the Core Information Management System by a CHECK Service Provider (an “**IT Health Check**”):
         1. prior to it submitting the Security Management Plan to the Customer for an Accreditation Decision;
         2. if directed to do so by the Customer; and
         3. once every 12 months during the Call Off Contract Period.
      2. conduct vulnerability scanning and assessments of the Core Information Management System monthly;
      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 Information Management System to determine whether the vulnerability affects the Core Information Management System; and
      4. conduct such other tests as are required by:
         1. any Vulnerability Correction Plans;
         2. the ISO27001 certification requirements;
         3. the Security Management Plan; and
         4. the Customer following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

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

* 1. The Supplier shall provide the Customer with the results of such Security Tests (in a form approved by the Customer in advance) as soon as practicable, and in any case within 10 Working Days, after completion of each Security Test.
  2. In relation to each IT Health Check, the Supplier shall:
     1. agree with the Customer the aim and scope of the IT Health Check;
     2. promptly, and in any case no later than 10 Working Days, following receipt of each IT Health Check report, provide the Customer with a copy of the IT Health Check report;
     3. in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:
        1. prepare a remedial plan for approval by the Customer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:
           1. how the vulnerability will be remedied;
           2. the date by which the vulnerability will be remedied;
           3. the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Customer, include a further IT Health Check) to confirm that the vulnerability has been remedied;
        2. comply with the Vulnerability Correction Plan; and
        3. conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.
  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 Customer.
  4. The Customer shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 8.3, the Supplier shall provide the Customer with the results of such Security Tests (in a form approved by the Customer in advance) as soon as practicable, and in any case no later than 10 Working Days, after completion of each Security Test.
  5. The Customer and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information Management System and/or the Supplier's compliance with the Security Management Plan ("**Customer Security Tests**"). The Customer shall take reasonable steps to notify the Supplier prior to carrying out such Customer Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature of the Customer Security Test.
  6. The Customer shall notify the Supplier of the results of such Customer Security Tests after completion of each Customer Security Test.
  7. The Customer Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If a Customer Security Test causes Supplier Non-Performance, the Customer Security Test shall be treated as a Customer Cause for the purposes of Clause 40.1 of this Call Off Contract, except where the root cause of the Supplier Non-Performance was a weakness or vulnerability exposed by the Customer Security Test.
  8. Without prejudice to the provisions of Paragraph 8.3.3, 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 Customer of any changes to the Core Information Management System and/or the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Customer's prior written approval, the Supplier shall implement such changes to the Core Information Management System and/or the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Customer or, otherwise, as soon as reasonably possible.
  9. If the Customer unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the Security Management Plan in accordance with Paragraph 8.8 above, the Supplier shall not be deemed to be in breach of this Call Off Contract to the extent it can be shown that such breach:
     1. has arisen as a direct result of the Customer unreasonably withholding its approval to the implementation of such proposed changes; and
     2. would have been avoided had the Customer given its approval to the implementation of such proposed changes.
  10. For the avoidance of doubt, where a change to the Core Information Management System and/or the Security Management Plan is required to remedy non-compliance with the risk management documentation, the Baseline Security Requirements and/or any obligation in this Call Off Contract, the Supplier shall effect such change at its own cost and expense.
  11. If any repeat Security Test carried out pursuant to Paragraph 8.9 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Customer may terminate this Call Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 42.2 of this Call Off Contract.
  12. The Supplier shall, by 31 March of each year during the Call Off Contract Period, provide to the Customer a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:
      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 Call Off Contract; and
      2. the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

1. Vulnerabilities and Corrective Action
   1. The Customer and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Customer Platform Data.
   2. The severity of vulnerabilities for 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 Security Management Plan and using the appropriate vulnerability scoring systems including:
      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
      2. Microsoft’s ‘Security Bulletin Severity Rating System’ ratings ‘Critical’, ‘Important’, and the two remaining levels (‘Moderate’ and ‘Low’) respectively.
   3. Subject to Paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Core Information Management System within:
      1. 7 days after the public release of patches for those vulnerabilities categorised as ‘Critical’;
      2. 30 days after the public release of patches for those vulnerabilities categorised as ‘Important’; and
      3. 60 days after the public release of patches for those vulnerabilities categorised as ‘Other’.
   4. The timescales for applying patches to vulnerabilities in the Core Information Management System set out in Paragraph 9.3 shall be extended where:
      1. the Supplier can demonstrate that a vulnerability in the Core Information Management 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 timescales set out in Paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;
      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 Customer; or
      3. the Customer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.
   5. The Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Call Off Contract Period unless otherwise agreed by the Customer in writing.
   6. The Supplier shall:
      1. implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent Central Government Body;
      2. promptly notify NCSC of any actual or sustained attempted Breach of Security;
      3. ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
      4. ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Call Off Contract Period;
      5. pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Security Management Plan;
      6. from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent month during the Call Off Contract Period, provide the Customer with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the 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 and any failure to comply with the timescales set out in Paragraph 9.3 for applying patches to vulnerabilities in the Core Information Management System;
      7. propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;
      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 Information Management System); and
      9. inform the Customer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations.
   7. If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10, the Supplier shall immediately notify the Customer.
   8. If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Paragraph 9.3, such failure shall constitute a material Default and the Customer may by terminate this Call Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 42.2 of this Call Off Contract.
2. Malicious Software
   1. The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Customer Platform Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.
   2. If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Customer Platform Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
   3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 10.2 shall be borne by the Parties as follows:
      1. by the Supplier where the Malicious Software originates from the Supplier Software, the third-party Software supplied by the Supplier or the Customer Platform Data (whilst the Customer Platform Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Customer when provided to the Supplier; and
      2. otherwise by the Customer.
3. Breach of Security
   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 Security Management Plan.
   2. The security incident management process set out in the Security Management Plan shall, as a minimum, require the Supplier upon becoming aware of a Breach of Security or an attempted Breach of Security to:
      1. immediately take all reasonable steps (which shall include any action or changes reasonably required by the Customer which shall be completed within such timescales as the Customer may reasonably require) necessary to:
         1. minimise the extent of actual or potential harm caused by such Breach of Security;
         2. remedy such Breach of Security to the extent possible and protect the integrity of the Information Management System against any such potential or attempted Breach of Security;
         3. 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 Customer, acting reasonably, may specify by written notice to the Supplier; and
         4. prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure;
      2. as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Customer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Customer.
   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 Information Management System and/or the Security Management Plan with the Baseline Security Requirements and/or this Call Off Contract, then such action and any required change to the Information Management System and/or Security Management Plan shall be completed by the Supplier at no cost to the Customer.
   4. If the Supplier fails to comply with its obligations set out in this Paragraph 11, such failure shall constitute a material Default, which if not remedied to the satisfaction of the Customer, shall permit the Customer to terminate this Call Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 42.2 of this Call Off Contract .
4. Data Processing, Storage, Management and Destruction
   1. In addition to the obligations on the Supplier set out Clauses 35.2 and 35.5 of this Call Off Contract and Call Off Schedule 17 (Processing Data) in respect of Processing Personal Data and compliance with the DPA, the Supplier shall:
      1. Process Customer Platform Data only in the UK, except where the Customer has given its consent in writing to a transfer of the Customer Platform Data to such other country;
      2. on demand, provide the Customer with all Customer Platform Data in an agreed open format;
      3. have documented processes to guarantee availability of Customer Platform Data in the event of the Supplier ceasing to trade;
      4. securely erase any or all Customer Platform Data held by the Supplier when requested to do so by the Customer; and
      5. securely destroy all media that has held Customer Platform Data at the end of life of that media in accordance with any specific requirements in this Call Off Contract and, in the absence of any such requirements, as directed by the Customer.

**Annex 1: Baseline Security Requirements**

1. Security Classification of Information
   1. If the provision of the Services requires the Supplier to Process Customer Platform Data which is classified as:
      1. OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Customer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or
      2. SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Customer prior to receipt of such Customer Platform Data and the Supplier shall implement additional measures as agreed with the Customer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.
2. End User Devices
   1. The Supplier shall ensure that any Customer Platform Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Customer except where the Customer has given its prior written consent to an alternative arrangement.
   2. The Supplier shall ensure that any device which is used to Process Customer Platform Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: REDACTED TEXT.
3. Networking
   1. The Supplier shall ensure that any Customer Platform Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.
4. Personnel Security
   1. All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.
   2. The Customer and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Customer to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Customer Platform Data or data which is classified as OFFICIAL-SENSITIVE.
   3. The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Customer has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.
   4. The Supplier shall ensure that Supplier Personnel are only granted such access to Customer Platform Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.
   5. The Supplier shall ensure that Supplier Personnel who no longer require access to the Customer Platform Data (e.g. they cease to be employed by the Supplier or any of its Sub-Contractors), have their rights to access the Customer Platform Data revoked within 1 Working Day.
5. Identity, Authentication and Access Control
   1. The Supplier shall operate an access control regime to ensure:
      1. all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and
      2. all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.
   2. The Supplier shall apply the ‘principle of least privilege’ when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.
   3. The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Customer on request.
6. Audit and Protective Monitoring
   1. The Supplier shall collect audit records which relate to security events in Core Information Management System 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 Core Information Management System, 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 Platform Data.
   2. The Supplier and the Customer shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.
   3. The retention periods for audit records and event logs must be agreed with the Customer and documented in the Security Management Plan.
7. Secure Architecture
   1. The Supplier shall design the Core Information Management System in accordance with:
      1. the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: REDACTED TEXT;
      2. the NCSC "Bulk Data Principles", a copy of which can be found at: REDACTED TEXT; and
      3. the NSCS "Cloud Security Principles", a copy of which can be found at REDACTED TEXT and which are summarised below:
         1. "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;
         2. "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
         3. "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;
         4. "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;
         5. "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
         6. "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Customer Platform Data and/or the Customer System that those personnel be subject to appropriate security screening and regular security training;
         7. "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;
         8. "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-Contractors and other suppliers;
         9. "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Customer to securely manage the Customer's use of the Service;
         10. "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
         11. "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;
         12. "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;
         13. "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Customer with the audit records it needs to monitor access to the Service and the Customer Platform Data held by the Supplier and/or its Sub-Contractors;
         14. "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

**Annex 2: Security Requirements for Sub-Contractors**

1. Application of Annex
   1. This Annex applies to all Sub-Contractors that Process Customer Platform Data.
   2. The Supplier must:
      1. ensure that those Sub-Contractors comply with the provisions of this Annex;
      2. keep sufficient records to demonstrate that compliance to the Customer; and
      3. ensure that its Project Plan includes Deliverables, Milestones and Milestone Dates that relate to the design, implementation and management of any systems used by Sub-Contractors to Process Customer Platform Data.
2. Designing and managing secure solutions
   1. The Sub-Contractor shall implement their solution(s) to mitigate the security risks in accordance with the NCSC’s Cyber Security Design Principles REDACTED TEXT
   2. The Sub-Contractor must assess their systems against the NCSC Cloud Security Principles: REDACTED TEXT at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-Contractor must document that assessment and make that documentation available to the Customer on the Customer’s request.
3. Data Processing, Storage, Management and Destruction
   1. The Sub-Contractor must not Process any Customer Platform Data outside the UK. The Customer may permit the Sub-Contractor to Process Customer Platform Data outside the UK and may impose conditions on that permission, with which the Sub-Contractor must comply. Any permission must be in writing to be effective.
   2. The Sub-Contractor must securely erase any or all Customer Platform Data held by the Sub-Contractor when requested to do so by the Customer; and securely destroy all media that has held Customer Platform Data at the end of life of that media in accordance with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard, or an alternative agreed in writing by the Customer.
4. Personnel Security
   1. The Sub-Contractor must perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard is at REDACTED TEXT
   2. The Sub-Contractor must, if the Customer requires, at any time, ensure that one or more of the Sub-Contractor’s staff obtains Security Check clearance in order to Process Customer Platform Data containing Personal Data above certain volumes specified by the Customer, or containing Special Category Personal Data.
   3. Any Sub-Contractor staff who will, when performing the Services, have access to a person under the age of 18 years must undergo DBS checks
5. End User Devices
   1. The Sub-Contractor shall ensure that any Customer Platform Data stored (for any period of time) on a mobile, removable or physically uncontrolled device is encrypted. The Sub-Contractor must follow the Information Commissioner’s Office guidance on implementing encryption, which can be found at REDACTED TEXT
   2. The Supplier shall ensure that any device used to Process Customer Platform Data meets all the security requirements set out in the NCSC End User Devices Platform Security Guidance, which can be found at: REDACTED TEXT
6. Networking
   1. The Supplier shall ensure that any Customer Platform Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.
7. Patching and Vulnerability Scanning
   1. The Sub-Contractor must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.
8. Third Party Sub-Contractors
   1. The Sub-Contractor must not transmit or disseminate the Customer Platform Data to any other person unless specifically authorised by the Customer. Such authorisation must be in writing to be effective and may be subject to conditions.
   2. The Sub-Contractor must not, when performing any part of the Services, use any software to Process the Customer Platform Data where the licence terms of that software purport to grant the licensor rights to Progress the Customer Platform Data greater than those rights strictly necessary for the use of the software.

**Annex 3: Security Management Plan Template**

REDACTED TEXT