Home Office

Adult Victims of Modern Slavery Care Co-Ordination Services

SECURITY POLICY

1. Purpose of this document

1.1 The purpose of this document is to outline the security requirements and classification guidelines that apply to the Contractor and internal and external stakeholders delivering Services under the Adult Victims of Modern Slavery Care Co-Ordination Services as well as their Sub-contractors advisors, consultants and appointed professionals who store or process existing Adult Victims of Modern Slavery Care Co-Ordination Services information for the Authority's purposes. In addition, specific guidance is given on information Adult Victims of Modern Slavery Care Co-Ordination Services information assets which are created as part of the Authority's processes.

1.2 The security requirements and classification guidance are from the Authority's security policies that are formulated from the HMG Security Policy Framework which stipulates the baselines. This can be found at https://www.gov.uk/government/publications/security-policy-framework.

1.3 Any queries, updates or issues relating to this document should be referred to the Authority's Contract Manager in the first place.

1.4 Where any provision in this document conflicts with any other provision in the Contract, the provision in this document shall apply. If the parties to this contract wish to override the provisions of this document the prior approval of the Corporate Security Department should be obtained.

2. Introduction

2.1 All records created, used or held by Government Departments are deemed Public Records under the Public Records Acts and must be compliant with the relevant legislation and handled in accordance with appropriate information management principles.

2.2 In addition, Government information and materials must be protected if unauthorised disclosure would harm the interests of the nation. The UK Government's Security Classification (hereafter referred to as "**GSC**") comprises of three levels (OFFICIAL, SECRET, TOP SECRET) designed to help individuals determine, and indicate to others, the necessary controls required to prevent the compromise of sensitive government assets; primarily, but not exclusively, National Security assets. Whilst the SECRET and TOP SECRET classifications are focused on the protection of assets related to National Security, OFFICIAL covers the protection of other types of non-national security related data. This reflects the need to provide practical and flexible protection to data, such as, non-HMG, business, commercial, and personal data. Some data may be classed as OFFICIAL-SENSITIVE where appropriate additional handling controls are considered necessary to reinforce the "need to know" principle.

2.3 Applying a classification to an asset indicates its sensitivity, or confidentiality, and thus the level of protection required. In order to determine which classification is appropriate for the protection of an asset, the 'consequence of compromise' must be considered, to determine the asset value, and therefore the necessary controls and the classification. When assessing the value of an asset it will be necessary to consider the direct and indirect consequences of compromise in relation to a breach or loss of:

- **CONFIDENTIALITY:** The restriction of information and assets to authorised individuals.
- **INTEGRITY:** The maintenance of information systems and physical assets in their complete and proper form.
- **AVAILABILITY:** The continuous or timely access to information, systems or physical assets by authorised individuals.

2.4 Each classification tier requires safeguards which must be adopted whatever the subject matter; thus, documents classified because of their political or economic content require similar safeguards as defence information.

2.5 In relation to Victims of Modern Slavery Care Co-Ordination Services and Services, we create, use and store large amounts of information in both paper and electronic format. All information - however it is recorded - needs to be managed properly to ensure that it provides the greatest benefit as well as being protected from loss or unauthorised alteration or disclosure. The classification appropriate to an asset may alter through the passage of time.

2.6 The Contractor shall ensure that each individual and organisation processing information in relation to the Adult Victims of Modern Slavery Care Co-Ordination Services delivery is personally responsible for the information he or she works with and for ensuring that it is used properly, kept up to date, shared only with

those who have a right to see it ('Need to Know' principle), stored in accordance with its sensitivity and classification, and only retained for as long as it is actually needed.

CLASSIFIED MATERIAL

3 Protectively Marked Material from the Government Protective Marking System (GPMS) and alignment to the GSC

3.1 Some information will continue to carry a protective marking from the previous Government Protective Marking Scheme. There is no direct correlation between the two schemes but, Non-personal Information marked RESTRICTED, UK RESTRICTED, PROTECT – PERSONAL, UK PROTECT - PERSONAL, PROTECT and UK PROTECT should be protected in line with the controls for OFFICIAL. There is no UNCLASSIFIED within the new scheme.

3.2 It is the Contractor's responsibility to maintain knowledge of all existing Adult Victims of Modern Slavery Care Co-Ordination Services information assets in the Contractor's possession that have been protectively marked: RESTRICTED, UK RESTRICTED, PROTECT – PERSONAL, UK PROTECT - PERSONAL, PROTECT and UK PROTECT, and for maintaining that protection in accordance with the guidelines set out in this Security Policy.

3.3 It is the Contractor's responsibility to maintain knowledge of all existing Adult Victims of Modern Slavery Care Co-Ordination Services information assets in the Contractor's possession that have been classified as OFFICIAL and / or OFFICIAL-SENSITIVE. Note OFFICIAL information does not need to be marked. Markings should, however, be applied to information classified as OFFICIAL-SENSITIVE.

4 Review of existing Classification and Downgrading

4.1 Once a classification has been assigned, 'information' will normally retain this classification until it is destroyed. Only the originator can classify an asset or change its classification, though holders of copies may challenge it with a reasoned argument. Where the originating organisation has ceased to function, its successor becomes responsible. Where a successor cannot be traced, the holder of a copy document may change its classification only after consultation with all other addressees.

4.2 This policy shall be reviewed ½ yearly by the Authority's Contract Manager to ensure that the classification scheme continues to comply with the SPF and the Authority's policy. Amendments to the classification scheme should be made and communicated to all parties.

4.3 For practical reasons, including the inability for parties to the Authority to modify existing Adult Victims of Modern Slavery Care Co-Ordination Services documents which are potentially disclosable, the Home Office does not presently propose to review all of the existing Adult Victims of Modern Slavery Care Co-Ordination Services material with a view to applying the new GSC. However, an appropriately authorised individual (i.e. a member of the Corporate Security Directorate) may elect to do so provided the rules of disclosure are adhered to. In the event that a review of existing classified material is undertaken, the correct classification should be determined in accordance with the guidance set out in this Security Policy relating to newly created material. It is not anticipated that any such review will be undertaken by external parties to HMG.

4.4 The Contractor must keep records which demonstrate that they have complied with the obligation to review their policy for the classification and downgrading of information held in pursuance of their obligations under Adult Victims of Modern Slavery Care Co-Ordination Services at least once every six months. Such records must be made available for inspection by the Authority on request within five working days of such a request.

5 Adult Victims of Modern Slavery Care Co-Ordination Services documentation created or owned by Agencies or Departments

5.1 Any existing Adult Victims of Modern Slavery Care Co-Ordination Services pertinent to information originating from other Agencies, or containing information relating to other Agencies or Departments, must be reviewed by the Contractor with the relevant Agency or Department before any changes to classifications are applied. As such, classifications applied by Agencies are unaffected by the guidance on the classification review set out in this Security Policy.

5.2 Agencies or Departments shall be informed and consulted by the Contractor on the process the individual is undertaking to review the classification of Adult Victims of Modern Slavery Care Co-Ordination Services information. The Contractor must retain records to demonstrate that the relevant Agencies and Departments have been consulted prior to the reclassification or downgrading of the classification applied to services,

documents and information created or received in pursuance of their duties under Adult Victims of Modern Slavery Care Co-Ordination Services. Such records must be made available for inspection by the Authority on request within five working days of such a request.

CREATION OF NEW DOCUMENTATION IN PREPARATION FOR CONTRACT MOBILISATION

6 Classifying HMG Information

6.1 The Contractor is responsible for ensuring that any new documentation created in preparation for the Authority which contains an information asset(s) is protected in accordance with the guidance set out in this Security Policy.

6.2 The Contractor shall treat any new documentation created pursuant to paragraph 6.1 as OFFICIAL unless instructed otherwise. Even though information classified as OFFICIAL is not marked as such, the 'need to know' principle set out in paragraph 2.6 above shall always apply.

6.3 The Authority does not envisage that it will be necessary to create any new documents which need to be classified as SECRET or TOP SECRET. However, if this does arise, the Contractor is obliged to advise the Authority for direction.

SECURITY AND STAFF VETTING REQUIREMENTS FOR ACCESS TO OFFICIAL MATERIAL

7 Organisation security controller

7.1 A Security Controller, with responsibility for day to day aspects of security must be nominated by the Contractor to be the contact for the Authority's Contract Manager (paragraph 1.3 above refers) together with a board level contact who accepts responsibility for security on behalf of the Contractor and to whom the Security Controller will report.

7.2 The Security Controller shall establish processes to ensure the full implementation of this Security Policy and that any breach or attempted breach of the requirements set out in this Security Policy, including attempts at manipulation or deliberate erasure or modification of records, must be reported within 24 hours or such earlier time if possible to the contact point at paragraph 1.3 above.

8 Clearance and Staff Vetting requirements for individuals accessing Adult Victims of Modern Slavery Care Co-Ordination Services information (including Sub-Contractors)

8.1 Security clearances held by individuals requiring access to Adult Victims of Modern Slavery Care Co-Ordination Services information assets which are classified OFFICIAL shall be at 'Baseline Personnel Security Standard' (BPSS) unless the information or assets is considered to be of value to terrorists or foreign intelligence agencies, in which case Counter Terrorism Check (CTC) will be required. Access to many Government buildings will fall under this provision. For the purposes of the services provided under the contract to supply Adult Victims of Modern Slavery Care Co-Ordination Services information assets are defined as a piece of information, stored in any manner, which is of value to the Authority or which carries a classification specified by the Government Classification Scheme as listed in paragraph 2.2 of this Security Policy.

8.2 The nature of the Authority's business is such that it conducts additional pre-employment checks on those wishing to work within Authority premises or be in receipt of, and / or work with, any equipment and / or information assets supplied by the Authority. The Authority reserves the right to refuse employment to those persons who fail these additional pre-employment checks.

8.3 A failure to pass these pre-employment checks will mean that the individual to whom the failure relates will not be permitted to work in any Authority premises or be able to access or work with any equipment or information assets supplied by the Authority or any equipment or information assets created as a result of Adult Victims of Modern Slavery Care Co-Ordination Services.

8.4 The Security Controller must report to *the Contract Manager* matters in relation to poor finance or criminality in relation to the Contractor's staff engaged in the delivery of the Services. Poor finance relates to instances where expenditure in providing Adult Victims of Modern Slavery Care Co-Ordination Services which is to be recovered in fees from the Authority can be demonstrated, through contract reviews, internal audit, external audit, whistle blowing or any other source, to be higher than would reasonably be expected had the Adult Victims of Modern Slavery Care Co-Ordination Services been subject to rigorous management and cost

control by the Contractor. Criminality refers to any act which may constitute a criminal offence under the laws in place, at the time that the services were discharged, in England and Wales, Scotland and Northern Ireland.

8.5 The security clearances at paragraph 8.1 above are set out in the Cabinet Office's "HMG Baseline Personnel Security Standard Guidance on the pre-employment screening of civil servants, members of the armed forces, temporary staff and government contractors", version 3 dated October 2013 or such updated version, as may be published from time to time https://www.gov.uk/government/publications/security-policy-framework. The Contractor shall comply with the requirements of the standard in full including the checks applicable to civil servants (which also require e.g. that individuals are commonwealth citizens or nationals of any of the member states of the European Economic Area (EEA), Switzerland and Turkey).

8.6 The Contractor shall ensure that individuals with access to Adult Victims of Modern Slavery Care Co-Ordination Services information assets shall have identity and immigration history checks carried out by the Authority. The information gathered by these checks may be used for the investigation of potential corruption and criminal activity. These checks will be commissioned by the Home Office Corporate Security Directorate (CSD) during the clearance process.

8.7 The Contractor shall ensure that individuals with any adverse outcomes, such as an adverse immigration history, convictions whether spent or not, may only have access to Adult Human Trafficking Victim Care Co-Ordination Services information assets with the prior written approval of the Authority. Such approval, if provided, shall be at the Authority's sole discretion only.

8.8 The Contractor shall ensure that individuals may not otherwise have access to HMG owned information except where there is a need for that individual to access in accordance with the Adult Victims of Modern Slavery Care Co-Ordination Services process. In that case, the individual may access the information providing they have the required minimum clearance, usually BPSS, or where access to the Authority's buildings is required, CTC. To maintain continued access, any queries from CSD in respect to the individual's clearance application must be resolved by the individual within five working days. In addition, any relevant business visa conditions for non-EEA nationals must be met before the individual starts work in the UK.

8.9 The Contractor shall ensure that individuals permitted access to classified material must be warned against divulging it to any unauthorised person and must be informed that the Official Secrets Acts 1911-1989 applies to them.

9 Physical Security of Adult Victims of Modern Slavery Care Coordination Services data

9.1 A layered approach to physical security on site should be adopted on a risk assessment basis. Physical security describes a range of controls that are intended to protect individuals from violence; prevent unauthorised access to sites and / or classified material (and other valuable assets); and reduce the risk a range of physical threats and mitigate their impact to a levels that is acceptable to the organisation. Security must be incorporated into the initial stages of policy, selecting, designing or modifying any building or facility, using appropriate methodologies; putting in place integrated and proportionate control measures to prevent, deter, detect and/or delay attempted "physical attacks", and to trigger an appropriate response.

9.2 Physical security measures should complement other technical, personnel and procedural controls as part of a "layered" or "defence in depth" approach to security that effectively balances prevention, detection, protection and response. For example, perimeter fencing and access control measures may deter an attack because of the difficulties of gaining access; CCTV or intruder alarms might detect an attack in progress and trigger interception; whilst vehicle stand-off, blast resistant glazing and postal screening can minimise the consequences of an attack.

9.3 The Contractor shall ensure that when not in use, OFFICIAL and OFFICIAL-SENSITIVE information assets must be stored securely in appropriate secure cabinets under lock and key or digital locks.

10 Computer Security

10.1 OFFICIAL Information assets must not be generated, stored, processed or transmitted on/from any computer system and/or network unless it has been approved for use by the Authority and/or an Accreditor. Consideration must be given to the protection of classified data whether on magnetic media or within the machine or network. This may mean stand-alone PCs or segregated networks with removable hard disks confined to a secure area with access controls for either approach.

10.2 The use of removable media must be minimised and approved by the Authority. Other approved information exchange mechanisms should be used where available. The amount of information moved to or transferred

using removable media must be minimised to the extent required to support the business requirement. Consider appropriate encryption to protect the content, particularly where it is outside the organisation's physical control. The minimum requirement for OFFICIAL-SENSITIVE information is Foundation Grade Encryption commercial encryption to FIPS-140-2 or equivalent may be acceptable with the prior written approval of the Authority and/or an Accreditor. Foundation Grade Encryption is linked to Commercial Product Assurance by the Government's Communications and Electronic Security Group. Commercial Product Assurance Certification can be awarded to any security-enforcing product, such as firewalls, virtualisation products and cryptography. A security product that is successfully assessed is awarded Foundation Grade Certification. This means the product has been proved to demonstrate good commercial security practice, and is suitable for lower threat environments. CPA allows products to be updated during the lifetime of certification as vulnerabilities and updates are required.

10.3 Appropriate safeguard, management and systems controls and audits must be in place to prevent the loss, theft of Authority assets. In the event of such a loss, the audits must clearly identify the complete audit trail in relation to that asset – for example, among other things audits must include details as to whom, where and when a person has access to the data, has viewed it, printed it, copied it or sent it by email.

11 Accreditation

11.1 It is a Mandatory requirement of the SPF that:

- All ICT systems that handle, store and process HMG information or business critical data, or that are interconnected to cross-government networks or services (e.g. the Public Service Network, PSN), must undergo a formal risk assessment to identify and understand relevant technical risks; and
- must undergo a proportionate accreditation process to ensure that the risks to the confidentiality, integrity and availability of the data, system and/or service are properly managed.

11.2 To gain the accreditation referred to at paragraph 11.1, the Contractor must ensure that the solution is appropriately accredited in accordance with the SPF using HMG IS1 and 2 and any supporting policies and documents. The Contractor will maintain the solution in accordance with the latest versions of the SPF, HMG standards and supporting policies and documents. Some environments may not need to be formally accredited. The Authority's Accreditor will advise on the appropriate level of assurance required in all cases.

12 Off-shoring

12.1 "Off-shoring" means any arrangement where data handling services or an element of services are performed outside the UK, as well as the more traditional offshore outsourcing arrangements (where whole business functions are carried out outside the UK). If there is any conflict between this security policy and the main contract over off-shoring issues the Authority's Corporate Security Department should be consulted over which document should take precedence.

12.2 If there is the potential for personal or other sensitive non-personal information to be held, processed or otherwise transferred outside the UK, the Contractor shall:

- Comply with the Authority's mandatory policy for Off-shoring proposals which will be made available to the Contractor following award of contract;
- Comply with the minimum mandatory measures (HMG IA Standard No. 6) set out in the data handling review http://www.iastandards.co.uk/;
- Have the Authority's Senior Information Risk Owner's (SIRO) assurance that adequate information risk assessment and protection is in place; and
- Ensure off-shoring of information that relates to or supports National Security is prohibited.

12.3 For personal data which is sensitive the Contractor shall additionally:

- Show evidence of a robust risk assessment of information risk;
- Take specific account of the legislative framework of the hosting country, particularly overriding provisions which may create tensions and potential conflicts with UK laws;
- Be sufficiently flexible to maintain a strong negotiating position, and include standard ERG contract clauses;
- Ensure that access, and the ability to copy or store records, is strictly limited to that required by business need; ensure that vetting of employees is appropriate for the data being handled; and that mitigation is in place for any other risks around employees of the off-shored site;
- Have robust independent assessment of supplier compliance with all arrangements contractual or otherwise; and

- Ensure any personal data held off-shore should be kept within the EEA, Safe Harbour or the limited number of countries with positive findings of adequacy from the European Commission.

12.4 A submission to offshore any part of the services under the contract(s) governing the Adult Victims of Modern Slavery Care Co-Ordination Services would need to be prepared for approval from the Authority's SIRO and then the Office of the Government SIRO. All submissions should be in consultation with the Authority CSD.

13 Transmission of classified material within the UK by post, hand, fax and e-mail

13.1 OFFICIAL Information assets may be sent by Royal Mail or an approved courier in a single envelope, never mark the classification on the envelope and include a generic return address on the reverse. Consider using registered Royal Mail service or reputable commercial couriers 'track and trace' service.

13.2 OFFICIAL-SENSITIVE Information assets should be protected by a double envelope may be sent by Royal Mail. However, never mark the classification on the outer envelope and include a generic return address. Consider using a Registered Royal Mail service or reputable courier equivalent where appropriate.

13.3 OFFICIAL information that does not contain any personal or sensitive content may be faxed within Great Britain. It may be faxed to/from Northern Ireland provided it does not contain any material about members or operations of the security forces. Care must be taken to ensure that the correct fax number of the addressee has been dialled before transmission begins. (This can be verified by sending a test sheet first and checking receipt whilst keeping the fax line open).

13.4 OFFICIAL information assets may be moved by hand between different UK sites or establishments but should be carried securely, preferably, in a sealed envelope inside a secure briefcase, box or pouch. A container of this kind should not be regarded as a security container and it, and the classified assets it contains, should remain in the possession of the individual at all times, unless it can be stored in an approved security container.

13.5 For all material, appropriate safeguard, management and systems controls - including division and oversight of responsibility - and audits must be in place to prevent the loss, theft or leak of personal data. In the event of such a loss, there must be a sufficient audit in place to clearly identify the complete audit trail in relation to that data – for example, audits must include details as to whom, where and when data has been accessed, viewed, printed, copied it or sent by email. In the event that an individual cannot show the audit, they become culpable for future handling of that data and document register.

13.6 If there is any conflict between this security policy and the main contract over the transmission of classified material within the UK the Authority's Corporate Security Department should be consulted over which document should take precedence.

14 Retention of classified material

14.1 The Contractor shall comply with the Authority's policies with regards to the retention of data/materials. A classification does not affect the length of time for which records must be held, this can depend on a number of reasons including whether the information needs to be held for statutory or regulatory (including audit) purposes.

14.2 The Contractor may contact the Contract Manager for confirmation/clarification on the retention policy of the Authority which will be supplied following award of contract.

15 Destruction of classified or material within the United Kingdom

15.1 As soon as they are no longer required, OFFICIAL HMG information assets must be disposed of in such a way as to make reconstitution unlikely. Shredding must be by an approved cross-cut shredder such that no more than two adjacent characters are legible in the shred size, and must be shredded to a length of no more than 15mm and a width of not more than 4mm. These baseline measures assume a font size no smaller than 12. Routine or regular use of font sizes smaller than 12 will require smaller shred sizes. Guidance about the physical destruction of assets is available in 'CPNI Requirements for Secure Destruction', March 2013 http://www.cpni.gov.uk/advice/Physical-security/secure-destruction-of-sensitive-items. Electronic media used to process HMG assets must be sanitised and disposed of in accordance with the requirements in 'HMG IA Policy No. 5 - Secure Sanitisation' http://www.iastandards.co.uk/;.

16 Loss of or Unauthorised Access to classified material

16.1 Any loss of HMG Information Assets (determined in accordance with this Security Policy), or the suspicion of unauthorised access to such material by the Contractor, their employees, suppliers, sub contractors or other party with whom they have shared HMG information assets, must be reported without delay to the nominated Contract Manager, who will liaise with the Corporate Security Directorate in the Home Office.

16.2 The Contractor shall comply with the SPF and the Authority's policy in relation to leaks, breaches and data incidents – a copy of which will be supplied at the start of the contract. Any such incidents must be immediately reported to the Contract Manager who will liaise with the Contractor's appointed Security Controller.

17 Quality control checks

17.1 The Contractor shall propose for the Authority's written approval, a suitable programme for the quality control of the information and the work completed on behalf of the Authority prior to the commencement of work. To reassure the Authority that services are being undertaken in a manner consistent with the Contract, an acceptable programme is likely to entail the Contractor undertaking a regular dip sample of letters and phone calls made and casework undertaken. The Contractor shall provide a Key Personnel to be responsible for this quality control work. The Authority shall be entitled to request all information relating to this quality control work at any time during or after the duration of the Contract and the Contractor shall provide a response within one week.

18 Access to the Casework Information

18.1 If access to Casework Information and other immigration message flows (including the Casework Information Database) is required for the discharge of services under Adult Victims of Modern Slavery Care Co-Ordination Services the Contractor will, for security purposes, be restricted and monitored to enable the relevant work to be completed but to prevent the potential for fraudulent or inappropriate or incorrect updates to the database.

19 Civil Service Code

19.1 The Contractor and those employed by the Contractor on this Contract will adhere to the Civil Service Code http://www.civilservice.gov.uk/about/values. Training must be conducted by the Contractor to ensure all Contractor staff are compliant with Authority's Security Policy.

20 Subcontractors

20.1 The Contractor must ensure that its Sub-contractors comply with all requirements within this Security Policy. The Contractor must ensure the appropriate integrity measures are in place in relation to their Sub-contractors and they must follow the general requirements for the Contractor as listed within the Security Policy in addition to undertaking the HADRIAN self assessment. The Authority will consider an onsite audit of the Sub-contractors in accordance with the provisions of this paragraph. HADRIAN is a self assessment facility used by the Authority which is designed to ensure that their supply chain and delivery partners are handling the Authority's data and assets in a manner that is compliant with Government security requirements, principally the Cabinet Office Security Policy Framework.

21 Retention of Documents and Right of Audit

21.1 The Contractor shall adopt a system of "open book" accounting and shall at all times:

a) maintain a full record of particulars of the cost of performing the obligations of the Contractor under this Contract (on a Business Unit basis), including those relating to the provision of services detailed in Schedule 02 Authority Requirements and

b) when requested by the Authority, provide a summary of any of the costs referred to in paragraph a) above, including details of any funds held by the Contractor specifically to cover such costs, in such form and detail as the Authority may reasonably require, together with ex Policy actions as required by the Authority, to monitor the performance by the Contractor of its obligations under this Contract; and

c) prepare any such accounts or other financial documentation as may be required by the Authority using the Historic Cost Convention and apply the four principles of prudence, going concern, consistency and matching; and,

d) provide such facilities as the Authority may reasonably require for its representatives to have access to all relevant staff, personnel, premises and records and visit any other place where the records are held and examine the records maintained under this paragraph.

21.2 For the purposes of this Security Policy Framework, Historic Cost Accounting is defined as the recording of all transactions made, and assets procured and liabilities obtained, in pursuance of the Adult Victims of Modern Slavery Care Co-Ordination Services at their nominal or original cost when either made, incurred or acquired

21.3 Compliance with paragraphs 21.1 and 21.2 above shall require the Contractor to keep (and to procure that the Principal Subcontractors shall keep) books of account on an "open book" accounting system and in accordance with best accountancy practice with respect to this Contract showing in detail:

a) all accounting policies used;
b) direct labour and indirect labour costs;
c) direct materials and Subcontract costs;
d) overhead costs analysed to identify appropriate categories such as administration;
e) payment details to suppliers and Subcontractors;
f) such revenue expenditure as not detailed above;
g) details of all accruals, prepayments, provisions;
h) details of all accounting adjustments and journal entries made;
i) such other available items relating to the Contractor's costs, income and profit as the Authority may reasonably require; and
j) such other items as the Authority may reasonably require to conduct cost audits for verification of cost expenditure or estimated expenditure, [as above and Schedule of any reference to Change Control or Official Secrets Act in this Security Policy.

21.4 The use of Fair Value Accounting or Mark to Market Accounting is not permitted. Fair Value Accounting is defined as any system of accounting which records transactions, assets and liabilities at an amount for which these could be exchanged between knowledgeable and willing parties in an arms length transaction.

21.5 The Contractor shall have (and procure that the Principal Subcontractors shall have) the books of account evidencing the items listed in Conditions Paragraph 21.3 available for inspection by the Authority (and any expert) upon reasonable notice, and shall present a report of these to the Authority as and when requested.

21.6 For the purposes of the National Audit Act 1983 the Controller and Auditor General may examine such documents as he may reasonably require which are owned, held or otherwise within the control of the Contractor and any Subcontractor and may require the Contractor and any Subcontractor to produce such oral or written explanations as he considers necessary. For the avoidance of doubt, it is hereby declared that the carrying out of any examination under Section 6(3) (d) of the National Audit Act 1983 in relation to the Contractor is not a function exercisable under this Contract.

21.7 If there is any conflict between this security policy and the main contract over the retention of documents and the right to audit the Authority's Corporate Security Department should be consulted over which document should take precedence.

22. Fraud and Corruption during the contract period

22.1 The Contractor is required to put in place appropriate counter-fraud and security management arrangements prior to the commencement date of the Contract. Within one month of the service starting, the Contractor must undertake a risk assessment of its counter-fraud and security management arrangements. The risk assessment should be provided to the Authority for consideration by a nominated counter-fraud specialist.

22.2 Allegations of corrupt activity received by the Contractor in relation to the service delivered for the Authority must be copied immediately to Home Office, Corporate Security Directorate. The Contractor must appoint a single point of contact in relation to investigation matters.

22.3 Independent systems must be in place to report whistle-blowing allegations. All Contractor staff should be provided with the direct line of the relevant team of counter-fraud specialists for the Authority.

22.4 The Contractor's staff are required to co-operate fully with any investigation into fraud or corruption. Fraud investigators appointed by the Authority must be given full and immediate access to all relevant personnel, premises, systems and records held by the Contractor and to their staff. The Authority shall have the power at any time during the provision of the Services to give the Contractor immediate notice requiring the removal from the Contractor's premises of any equipment, documentation or other evidence which, in the reasonable opinion of the Authority's Representative is required as evidence of part of an investigation.

23. Prevention of Corruption prior to Award of Contract

23.1 The Contractor shall not do (and warrants that in entering this Contract it has not done) any of the following:

a) offer, give or agree to give any employee or representative of the Authority or the Crown any gift or consideration of any kind as an inducement or reward for doing or refraining from doing (or having done or refrained to do) any act in relation to the obtaining or performance of this Contract or any other Contract with the Crown; or
b) enter into this Contract or any other contract with the Crown in connection with which commission has been paid (or agreed to be paid) on the Contractor's behalf or with its knowledge unless, before the Contract was signed, particulars of the commission were disclosed in writing to the Authority.

23.2 Where the Contractor (or a Principal Sub-contractor or member of the Contractor's Staff or anyone acting on its behalf) commits or has committed any act or omission referred to in Condition in Paragraph 23.1 or any offence under the Bribery Act 2010 in relation to this or any other contract with the Crown (the "Prohibited Act") the Authority has the right, subject to Condition in Paragraph 23.2 (a,b,c below) to:

a) terminate the Contract and recover from the Contractor the amount of any loss resulting from the termination; or
b) instruct the Contractor to terminate the Principal Sub-contractor with immediate effect; and
c) recover from the Contractor any other loss sustained in consequence of any breach of this Condition whether or not the Contract has been terminated or whether or not a Principal Sub-contractor has been terminated.

23.3 If the Prohibited Act (defined as any act contrary to civil and criminal law in England and Wales, Scotland and Northern Ireland or any act contrary to the provisions of the Civil Service Code) is committed by an employee or director of the Contractor acting independently of the Contractor or by a Subcontractor (or anyone working for it) then the Contractor may within twenty (20) Working Days of the Authority or the Contractor becoming aware of the Prohibited Act dismiss that employee or terminate or procure the termination of the relevant Subcontract and provided that it:

- is able to demonstrate to the Authority's reasonable satisfaction that it will be able to continue to deliver the Services notwithstanding such dismissal or termination; and
- compensates the Authority for any losses suffered as a result of the Prohibited Act,

then the Authority shall not have the right to terminate this Contract pursuant to Condition in 23.2, a) "terminate the Contract and recover from the Contractor the amount of any loss resulting from the termination".

24 Business Continuity and Disaster Recovery

24.1 The Contractor shall put in place an effective and up-to-date Business Continuity Management (BCM) system to maintain or else quickly resume provision of key services in the event of a disruption. BCM arrangements must follow industry best practice (BS25999 or equivalent standard). This includes disaster recovery Policies for key ICT systems, along with appropriate arrangements to minimise the impact of a terrorist attack or other critical incidents.

24.2 The Contractor is required to produce, prior to the Contract Effective Date, a comprehensive Business Continuity Plan ("BCP"), including Disaster Recovery procedures which meets the British Standard for Business Continuity Management, BS25999. The BCP shall be agreed by the Authority, which shall not unreasonably withhold its approval.

24.3 The BCP should be written to complement the phases of the Contract which are:

- mobilisation
- delivery and execution
- exit and handover.

24.4 The situations in which the BCP can be utilised should include as a minimum:

- General
- Destitution
- Denial of access to premises

- Loss of Communications systems, recording systems;
- Denial of access to personnel including such instances as a serious adverse weather event or travel disruption;
- Resourcing of the contract (staff, systems and all premises including but not limited to outlets).
- IT and Security
- Loss of Authority Data
- Breach of IT and Security requirements

24.5 The BCP shall include the critical activities to be recovered and the Key Representatives responsible, including but not limited to:

- Procedures for invocation of the plan including those with authority to invoke.
- Key contact details for both the supplier and customer.
- The timescales in which the critical activities are to be recovered.
- The recovery levels needed for each critical activity.
- The resources required to achieve the defined recovery levels.
- Strategies for recovery.

24.6 The Contractor shall ensure that the BCP complies fully with Clause ** of the Contract, Schedule 2 (Statement of Requirements) and Schedule 10 (Security Requirements and Plan).

24.7 The Contractor shall ensure that it's Staff and it's Sub-Contractors' staff have access to a copy of the BCP and are trained in these emergency procedures and understand their roles and responsibilities if the plan is invoked.

24.8 The Contractor shall ensure that all of its staff, whether directly employed or via a Sub-Contractor, understand the manual back up of the systems in place to ensure that, in the event of any failure to its IT systems used in the delivery of the Services, it is able to carry out the Services with minimal disruption.

24.9 The Contractor shall ensure that the risk assessments which inform the BCP and the BCP itself are regularly refreshed and updated as appropriate and no less than once every six months. Any changes to the BCP need to be approved by the Authority as part of the strategic review meetings which form part of the contract management regime, as set out in Schedule 14 (Contract Management Regime).

24.10 The Contractor shall ensure the BCP is subject to regular testing, at a minimum this should occur annually or following a significant change in processes, staff or technology. The Contractor should issue a report to the Authority highlighting any failures in the BCP revealed by the test and proposals for remedying any failures. The Contractor shall promptly implement any actions or remedial measures which the customer considers necessary as a result of those tests.

24.11 If there is any conflict between this security policy and the main contract over business continuity the Authority's Corporate Security Department should be consulted over which document should take precedence.