Schedule 16 (Security)

Part A: Short Form Security Requirements

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Schedule 1 (Definitions):

"Breach of Security" the occurrence of:

a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or

b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,

in either case as more particularly set out in the Security Policy where the Buyer has required compliance there with in accordance with Paragraph **Error! Reference source not found.**;

"Security Management Plan" the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.

2. Complying with security requirements and updates to them

2.1 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.2 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.3 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.4 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

3.2.4 where specified by the Buyer in accordance with Paragraph **Error! Reference source not found.** complies with the Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in Paragraph **Error! Reference source not found.** shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

4.1 Introduction

4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

a) comply with the principles of security set out in Paragraph **Error! Reference source not found.** and any other provisions of this Contract relevant to security;

b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer’s Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer’s Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with the Security Policy as set out in Paragraph **Error! Reference source not found.** ; and

g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 Development of the Security Management Plan

4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph **Error! Reference source not found.**, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph **Error! Reference source not found.**, or any subsequent revision to it in accordance with Paragraph **Error! Reference source not found.**, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph **Error! Reference source not found.**. However, a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph **Error! Reference source not found.** shall be deemed to be reasonable.

4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph **Error! Reference source not found.** or of any change to the Security Management Plan in accordance with Paragraph **Error! Reference source not found.** shall not relieve the Supplier of its obligations under this Schedule.

4.4 **Amendment of the Security Management Plan**

4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

a) emerging changes in Good Industry Practice;

b) any change or proposed change to the Deliverables and/or associated processes;

c) where necessary in accordance with Paragraph **Error! Reference s ource not found.**, any change to the Security Policy;

d) any new perceived or changed security threats; and

e) any reasonable change in requirements requested by the Buyer.

4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include:

a) suggested improvements to the effectiveness of the Security Management Plan;

b) updates to the risk assessments; and

c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph **Error! Reference source not found.**, any change or a mendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph **Error! R eference source not found.**, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph **Error! Reference source not f ound.**, the Supplier shall:

5.2.1 immediately use all reasonable endeavours (which shall include any action or changes reasonably required by the Buyer) necessary to:

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

b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

c) prevent an equivalent breach in the future exploiting the same cause failure; and

d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with Paragraph **Error! Reference source not found.**) or the requirements of this S chedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

Part B – Annex 1:

Baseline security requirements

1. Handling Classified information

5.4 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

6. End user devices

6.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre (“NCSC”) to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").

6.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a ‘known good’ state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

7. Data Processing, Storage, Management and Destruction

7.1 The Supplier and Buyer recognise the need for the Buyer’s information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

7.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 18 (Data protection).

7.3 The Supplier shall:

7.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

7.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

7.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

7.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

8. Ensuring secure communications

8.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

8.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

9. Security by design

9.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

9.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

10. Security of Supplier Staff

10.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

10.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

10.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.

10.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

10.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

11. Restricting and monitoring access

11.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

12. Audit

12.1 The Supplier shall collect audit records which relate to security events in the systems 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:

12.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

12.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

12.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

12.3 The Supplier shall retain audit records collected in compliance with this Paragraph **Error! Reference source not found.** for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

31/07/2023

Job Information	
Job Code: P010585	Job Location: UK
Date Raised: 31st July 2023	Date Approved:
Assignment Version: 1.3	PiC: [redacted]

CONTENTS

1 INTRODUCTION

PA's security acumen is central to our growth ambitions. A single incident can undermine trust in our brand and tarnish all the good work that we do. It is therefore vital that our approach to security remains proportionate, holistic and focused upon thinking through the risks and delivering the right behaviours.

High profile security incidents have increased awareness of the range of threats businesses face and as we become more dependent upon technology, so the range of threats increases. PA is not immune from the prevailing threats and our work with very prestigious organisations means we must carefully evaluate the risks posed by individuals, international criminal groups or State-orchestrated actors. Our clients also have high expectations of us, and demand assurances that we have considered the risks and will safeguard their interests.

A thorough evaluation of the risks must be performed before an assignment commences and regular reviews undertaken throughout the lifecycle. Where the risks are greater than can be mitigated by PA's standard security arrangements (see section 4), an Assignment Security Plan is required, that details how the assignment team will protect people, data, intellectual property or any other assets.

Regardless of if the standard arrangements apply, it is the responsibility of the AM/PiC to ensure that their teams are briefed on them regularly, and where relevant a copy of the security plan is available on the commercial file for the assignment.

Our approach to Assignment Security

The assignment security processes continue to evolve to help safeguard PA, our people and our clients in response to the prevailing threats. PA's assignment security processes are designed to:

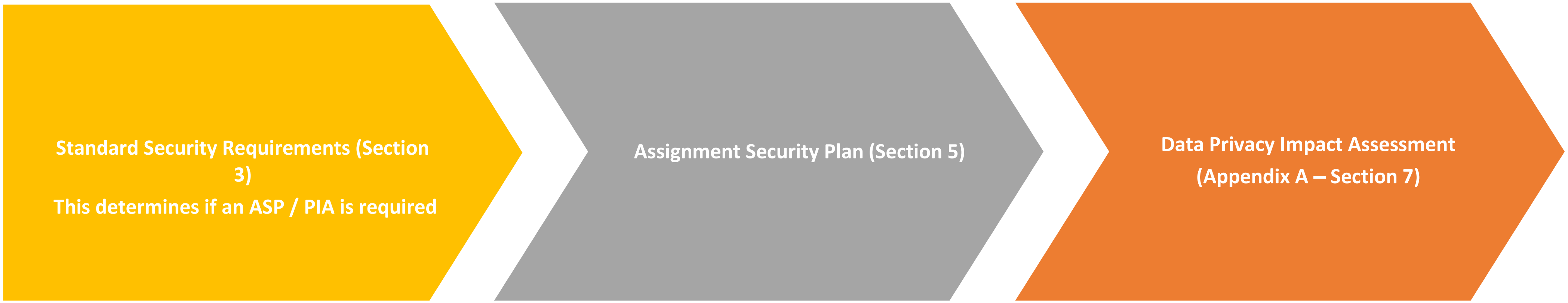
- help Assignment Managers to identify the security risks associated with client projects
- define working methods which will mitigate any risks
- identify any additional management controls required to meet existing PA and client security standards
- protect our reputation and our people

PA's standard security arrangements when implemented and adhered to properly, are adequate for most assignments. Where an assignment requires additional security measures an Assignment Security Plan (ASP) must be completed.

If an ASP is not required at the start of an assignment, Assignment Managers are responsible for the ongoing assessment of their assignment and for completing an ASP if the threats have changed.

Assignment Security Process Flow

An ASP is required where an assignment's risks are considered greater than can be reasonably mitigated by PA's standard security arrangements.



Standard Security Requirements (Section 3)

This determines if an ASP / PIA is required

Assignment Security Plan (Section 5)

Data Privacy Impact Assessment (Appendix A – Section 7)

It is mandatory for Assignment Managers to assess the security implications of their assignment by completing Section 3 of this document.

If an assignment includes the flow of personal data, then a Data Privacy Impact Assessment (DPIA) must also be completed.

2 ASSIGNMENT SECURITY PROCESS

2.1 Should I complete an Assignment Security Plan (ASP)?

It is mandatory for Assignment Managers to assess the security risks of their assignment before, during and at the end of an assignment.

An ASP must be produced if, having evaluated the assignment and weighed the risks to PA and our clients', the Assignment Manager or the client determines that PA's standard security arrangements are insufficient.

When an ASP is completed, there is a requirement for it to **be signed by the Partner in Charge and shared with the Client if appropriate** and stored on the assignment job site (commercial file) / PA SharePoint Online. It is incumbent on the Assignment Manager to ensure that all parties have a firm understanding of PA's obligations and capabilities, and that the team are 'signed up' to adopting and adhering to the appropriate behaviours to mitigate any risks.

Data Privacy Impact Assessment (DPIA/PIA)

PA may need to process personal data on behalf of clients in order to deliver the agreed engagement. When it is identified that personal data may be involved in an assignment, a DPIA (see Appendix A) must be completed prior to the commencement of the assignment and then reviewed at regular intervals thereafter.

3 standard SECURITY REQUIREMENTS

At the prospect stage of an assignment, the Assignment Manager/Partner in Charge will complete a risk evaluation in xRM. Throughout the lifecycle of the assignment, Assignment Managers must regularly review and update the risk assessment (shown below) to ensure risks are captured and mitigated appropriately.

Where it is determined that PA's standard security arrangements (detailed in section 4) are inadequate to mitigate the assignments risks, and further mitigations are needed, an Assignment Security Plan must be completed. The following assessment must be completed in xRM for new assignments, or for existing assignments where the risks have changed, the table below must be completed, and a copy stored on the job site.

The Assignment Manager is responsible for identifying any additional security measures required by highlighting the specific risk catagories - this governs which elements need to be risk assessed in section 5.

Assessment

Risk Considerations	Yes / No
Is Personal Data (PD) being handled during the assignment? For an explanation of PD click here if EU / here if USA or for further advice contact the legal team). If yes, **please complete a Data Privacy Impact Assessment** (Section 7.1 of this document) in addition to an Assignment Security Plan.	No
Does the work location require special consideration, personal safety (Section 4.8) or additional information security eg, travel to countries identified as Red or Amber on PA's list of countries (click here for countries lists or contact the Head of Security)	No
Do any conditions or methods of working agreed with the client require changes to standard PA information security arrangements, this includes assignments where any of the work is completed outside of the PA network? For example, **MS Teams**, the use of websites such as webmail, Gsuite or cloud storage sites such as Dropbox/Client SharePoint.	Yes
Are any government protectively marked documents handled during the assignment?	Yes
Are there other security considerations that need to be taken to account such as? • employing subcontractors • are PA teams delivering work from different legal jurisdictions? • is there a master service agreement with additional security requirements? • is there a framework agreement with additional security requirements? • does the assignment need an asset handling protocol?	Yes
Having evaluated the Health and Safety arrangements for the assignment in line with PA's H&S Policy, are there any areas of concern or risk regarding the H&S of PA people or our clients that may be affected by our activities, and that need	No

to be assessed and mitigated through a specific assignment H&S risk assessment? (For support contact the H&S coordinator who will help you through the exercise)	

If you are performing software/hardware development work, please tick this box and read document Annex B - DEVELOPERS GUIDE TO EMBEDDING GOOD SECURITY PRINCIPLES ☐

The link to document is here.

The following Section (4) details PA's standard security arrangements that apply to **all** PA assignments. **It is imperative that these standards are communicated and understood by all assignment team members.**

4 pa’S standard security arrangements

The security arrangements below represent PA’s **baseline standards** for assignment security and must be communicated to the assignment team (including contractors) at the start of an assignment and to any new team members when they join.

4.1 Protecting client and PA WORKSPACES

- Always follow the client’s security policies and procedures when on site unless PA’s policies, procedures or an Assignment Security Plan (when required) offer greater protection
- When on client site, check who is following you into access-controlled areas, ensuring that they are authorised to enter unescorted or, if not, that they are under escort by an appropriate person
- Wear your pass at all times. This confirms your entitlement to be in an area and saves the embarrassment of being asked to confirm your identity. When leaving buildings your pass should not be displayed and must be removed from view
- If a person is not wearing a pass in an access-controlled area and you are unsure of his/her authority to be there, challenge politely, ask to see their pass and request they wear it. If they are unable to produce a pass escort them out of the area
- Never leave visitors unattended in access-controlled areas.

4.2 Protecting access to information and Intellectual property

- Clear office policy: Outside normal working hours and during the working day, ensure that sensitive information or other items of value are appropriately secured and placed out of sight or in lockable cabinets. A clear desk demonstrates to clients that we take security seriously and that we are professional and can be trusted with their information
- If carrying confidential or sensitive information or intellectual property on public transport or in public areas, always keep it under direct control and supervision. When passing through airports, take particular care to ensure that such items are not mislaid
- Observe the relevant client rules and procedures in respect of different types of data, eg, personal data, government classified information or sensitive technical data and understand how it should be handled correctly
- When printing, scanning or copying documents, do not leave the documents unattended on the printer. Printed material must be handled and stored securely
- Do not discuss sensitive business issues in public areas in person or on the telephone where overhearing would risk unauthorised disclosure of privileged information
- When employing sub-contractors, ensure that they understand the local legal and regulatory requirements and the arrangements for privileged information
- When individuals, including sub-contractors, leave an assignment, **ensure they return or delete all assets** including client data, documentation and equipment.

4.3 Protecting access to IT systems and electronic information

- When working on your computer always lock the computer screen if the computer is unattended. Use a privacy screen if working in public spaces
- If carrying laptops, removable media, or work mobile phones on public transport or in other public areas, always keep them under direct control and supervision
- Passwords for computers/mobile phones must not be disclosed and must not be kept in written form in a place or manner that may allow unauthorised users to gain access
- Wherever possible, avoid taking your laptop to social occasions in public areas (e.g. restaurant/bar). If you have to take your laptop, do not leave it unattended for any reason
- Do not send business (assignment, client or general PA) emails to personal e-mail accounts unless you have been specifically authorised to do so. Auto-forwarding of emails is not permitted
- Connecting a PA laptop to a client network is not permitted. This measure is designed to protect both the client and PA. Similarly, client laptops cannot be connected to the internal PA network.

4.4 USE OF MICROSOFT TEAMS

This section only applies if you are using Teams to collaborate with third parties (clients, suppliers, guests). If you require a Teams site please contact the global help desk and also specify the domains you wish to share externally with. Domains are to be recorded in the ASP below. Please note that consumer domains, such as gmail.com, will not be permitted.

We have secured Teams to a certain level however, so we can continue to protect our firm from inappropriate data exposure, it is critical that access and usage is sensible and that you follow our policy. Our policy is that:

- each group has a Team owner (usually the assignment manager) who has responsibilities to:
  - ensure only those third-party people who need access are added to the Teams site. Note: an ‘allow list’ of a company/organisations domain will be added, not personal/consumer email address
  - ensure if someone leaves the third-party company, or no longer requires access, they are removed
  - brief all people working on the Teams site about their responsibilities
  - demonstrate who has accessed the site, if required
  - report any inappropriate usage of Teams to the Partner in Charge and/or Operational Risk.
- everyone who uses the Team (including team owners) is aware:
  - that documents with certain classifications (e.g. PA Internal Use) will be blocked from being shared with third-parties by Teams. Documents will need to be re-classified appropriately following the correct PA or client classification, they cannot be released
  - that when working with Teams that have third-party access enabled you need to take care not share content inappropriately
  - of any specific client contract or assignment restrictions (for example, accessing or storing content at home or from/on a non-PA device, this may not be allowed)
  - not to use Teams to gain access to other features and capabilities that you may become aware of without checking with the assignment manager.

4.5 Completing appropriate personnel security checks on our people

PA completes the appropriate baseline standards checks and due diligence on PA people and non-PA people such as contractors in all countries in which we operate.

If security clearances are required by the client, all members of the assignment team, (including subcontractors), must be security cleared to the level necessary for the assignment. Clearance must be obtained before access is given to client information. If further advice is required contact PA’s security vetting team on [redacted] or email Operational Risk.

4.6 SECURITY BRIEFINGS

Regular security briefings must be held during the assignment to:

- ensure that new team members are aware of security expectations
- confirm that current security arrangements continue to be appropriate for the assignment
- identify changes that require mitigation e.g. changes to master services agreements
- provide an opportunity to report/discuss security issues or breaches.

A positive approach to reporting possible security incidents is vital and should be focused on fixing the problem and not apportioning blame. The Assignment Manager (or person with delegated responsibility for assignment security matters) is responsible for briefing assignment team members on their security obligations at the start of an assignment and for updating the brief (every six months as a minimum, or when circumstances change).

Depending on the sensitivity of the assignment or the client, additional security measures may be necessary at the proposal stage. Security measures need to be recorded in this document and implemented once the bid is successful and assignment planning activities begin.

THE FIRST SECURITY BRIEFING

The initial briefing should, as a minimum, deliver the following security-related information to all members (PA/sub-contractor) of the assignment team:

- Nature and objectives of the assignment
- Key assets, dependencies and capabilities likely to be required to bring the assignment to a successful conclusion
- Main areas of potential security vulnerability e.g. threats and risks
- Standard security measures most relevant to the particular assignment and as appropriate, any enhanced security measures required for the assignment e.g. security clearance
- Aspects of the assignment where a greater level of security risk may have to be 'tolerated' (subject to Head of Security approval)
- What to do/how to report in the event of identifying a security concern or incident.

The briefings should be delivered verbally to permit questions and facilitate clarification where required. Assignment and ongoing briefings incorporating this plan will be completed and recorded in the assignment file together with acknowledgements from team members.

Subsequent briefings should take place either as a refresher (every six months) or following a security incident, other security event, or following changes in contractual or legal and regulatory law.

ALL briefings must have a written record in the form of either an attendance sheet or an email as confirmation. The records are to be stored with the job on the Teams site in Office 365 / other approved system along with this document.

4.7 REPORTING SECURITY INCIDENTS PROMPTY

Security incidents may occur from time to time and must be addressed at the earliest possible stage in any given part of the process. All assignment team members must be able to recognise where risk is or might be arising and must have sufficient awareness and knowledge of how to report and respond to security risk issues.

Any loss of assignment material outside the client location will be treated as a security incident and should follow the steps below:

Respond effectively to security concerns and incidents

In response to a security concern or incident, follow these four main steps:

1. identify and assess - make an appropriate inventory of any items judged to be lost or otherwise compromised, eg, hard copy documents, removable IT media, laptops
2. report - when reporting a security concern or incident, always ask yourself 'who needs to know?' As a minimum this must include the Assignment Manager
3. monitor - if you are the first to discover a concern or incident, continue to monitor and report until you know that responsibility has been assumed or the incident is closed

4. close - record lessons identified; implement and communicate any improvements as appropriate.

If you become aware of a security concern or incident do not assume that someone else is/will be dealing with it, always check. It may not always be obvious that a security lapse has occurred, and it is important to be able to recognise the signs.

A security concern or incident could be:

1. a person is found in possession of information, intellectual property, items of technology or IT to which he/she may not be entitled
2. information or other items of value have been tampered with or are lost
3. cabinets, desks or offices used to store privileged information are discovered open and unattended
4. an unfamiliar person in an access-controlled workspace looking lost or not wearing a pass being unduly inquisitive in areas or about matters which do not concern them
5. business information sent to personal e-mail accounts without prior authority.

Speak up if you have any concerns. If something feels wrong, report it to your Partner in Charge, Assignment Manager or project manager straight away. If the incident/risk severity is high and could damage the business in any way contact **Operational Risk** [redacted] **or Head of Security** [redacted] immediately.

4.8 REPORTING HEALTH AND SAFETY INCIDENTS PROMPTLY

In order to protect the wellbeing of our people we monitor all accidents and near misses. This information enables us to undertake investigations and put in place measures to prevent and mitigate the risk of recurrences. All accidents and near misses must be reported as soon as possible after the incident using the accident form (here) on PA's accident management system. This should be done by whoever is best placed to make the report but essentially it does not matter who, just that the incident is reported. The accident form can be found on PA H&S page on Office365. Once the form has been submitted, the H&S coordinator will begin the investigation and engage with the relevant parties within PA.

Please follow and adhere to PA's guidance in relation to the current Covid 19 pandemic.

If you have any questions about this process, please contact the H&S Coordinator.

4.9 ESSENTIAL INFORMATION WHEN TRAVELING ABROAD

The safety of our people is our highest priority, and our work often takes us away from home. Circumstances in the locations where we work can change, often rapidly. PA work with security and travel agencies to assess the threat factors in the countries where we operate in order to ensure that we are kept safe when working. Here is the current threat analysis for each country, and who to contact for further information and approval to travel to higher risk countries.

What to do in an emergency

When traveling on business, it is important to keep a note of the contact details of PA's Personal Accident and Travel Insurance provider. Assistance is available 24 hours a day, every day of the year.

Print a copy of this emergency card and keep it with you at all times.

To load the contact card, ctrl click on this here and save the details to your address book.

If you fall ill and need assistance or advice , call Zurich Travel Assistance - Call +44 (0)1489 868 888 or visit www.zurich.co.uk/travelassistance

The helpline is manned 24 hours a day, 365 days a year by multi-lingual assistance co-ordinators, experienced in managing medical assistance cases with hospitals and clinics worldwide. Also available are security experts to provide a comprehensive range of complementary security services.

- The insured person must contact Zurich Travel Assistance as soon as reasonable if illness or bodily injury results in the need for in-patient hospital treatment.

- Zurich will not pay for any emergency repatriation expenses incurred without the prior consent of Zurich Travel Assistance or for any hospital treatment provided on an in-patient basis where the insured person has not made all reasonable attempts to obtain the prior consent of Zurich Travel Assistance or obtained the consent of Zurich Travel Assistance as soon as reasonable.

- When seeking medical or travel assistance please make sure the following information is available:
  a) the insured person’s name
  b) the telephone or facsimile number where an insured person can be contacted;
  c) the insured person’s address abroad;
  d) the nature of the emergency or the assistance required;
  e) the name of the insured person’s company, employer or organisation.

If you require help/advice when planning to travel to an Amber or Red flagged country (see country list here), contact Lawrence Ward, PA’s Head of Security.

Visas and work permit

Before travelling please check whether there are visa or work permit requirements. Newland Chase are PA UK’s appointed immigration advisors who will manage the application process for you and will assist you with all your requirements. Please check with Newland Chase on a case-by-case basis before travelling as visa requirements are dependent on nationality, the country being visited, and the purpose of the visit. They can be contacted via our dedicated mailbox: [redacted] or on [redacted]

Embargoed Countries

The UK, EU and the US have sanctions in place which restricts our ability to work or contract in specific countries. There are significant penalties for violating such embargos, including imprisonment, and it is therefore vital to first check the current embargo restrictions here and to discuss with Group Legal as necessary.

4.10 CLOSING DOWN THE ASSIGNMENT UPON COMPLETION

At the end of the assignment a security handover must be completed with the client to ensure that any sensitive information is archived or disposed of securely as appropriate as per stage 5 of the PAAAS.

All data to be removed from PA laptops and stored on the Teams site in Office 365 / other approved system where appropriate.

Client Assets

If you are issued with client IT such as a laptop, phone or other media storage device, this must be recorded in the client file. It's status must be recorded when returned to the client so that there is a clear record of the custodian of any assets. When returned, a record and receipt must be kept (such as a courier receipt) as well as following any specific asset handling requirements from the client.

Confirmation of the above handover and the client’s approval must be recorded and uploaded to the job site (commercial file) / PA SharePoint Online.

ASSIGNMENT DEBRIEFING

Leavers (PA or subcontractors) must be debriefed when they leave the assignment, whether it is at the conclusion of the assignment or before. The purpose of this debrief is to:

- remind team members of their obligations relating to the privacy and security handling of data related to the assignment
- confirm that all client information held by the individual has been returned to PA, the client or destroyed as appropriate, and it has been removed from all laptops as required
- ensure that all hard equipment, access control passes, and removable media has been returned to its rightful owner.

Assignment debriefs will be conducted and recorded in the assignment file and assignment material will be archived or disposed of securely.

Confirmation of the above **must** be recorded and uploaded to job site (commercial file) / PA SharePoint Online.

5 assignment security plan (ASP)

An ASP must be produced if, having considered PA's and the clients' potential risks, the Assignment Manager or the client determines that PA's baseline measures are not sufficient.

*[NOTE: This section is not a standalone document and must include **all** previous pages]*

5.1 Assignments processing personal data

If you are processing personal data, you will also need to complete a Data Privacy Impact Assessment (appendix A).

It is a **legal requirement** that you complete this, and failure to do so could result in PA being subject to an external investigation and significant statutory fines.

5.2 Reviewing – ongoing Maintainance of high security standards

Once the ASP is approved and in place, the Assignment Manager is responsible for ensuring that the ASP remains up to date and continues to be relevant to the assignment. AM's can do this by:

- holding regular assignment team briefings to discuss the ASP with your assignment team and invite comment/collaboration on resolving any issues
- engaging with the client to ensure that they continue to be comfortable with the security arrangements in the ASP
- completing an annual document review of the ASP, or reviewing the ASP when the assignment changes significantly
- periodically auditing the assignment team to check they are complying with the ASP
- update the ASP if there are any relevant changes to the master service agreements or the framework agreement
- asking Operational Risk for help if additional guidance is needed.

Keeping the ASP updated ensures that PA and client information is protected and enables us to deliver against our objectives.

5.3 Assignment Security Plan

Assignment Synopsis

Why does this assignment require further security controls in addition to the baseline measures outlined in the assignment security process guidance?

1. This assignment requires PA members of staff to liase and work closely with people from different companies as the client has asked for the project to be delivered by a Consortium.
2. We will require a shared MS Teams site that can have external parties join from the following domains:

   [redacted]
3. DfE will share materials with us via an MS Teams site hosted on their network to which Consortium members will have access.
4. Design documentation as well as PMO material (progress reports, stakeholder list, project risk logs, programme plan, workshop presentations) will be stored and shared on the internal Microsoft Teams site. Anything confidential or commercially sensitive information will be saved under internal management site with limited access to identified PA employees.
5. We will use AirTable to track and communicate PMO material, programme status and reporting. Corporate information will also be tracked in the same platform.
   a. Airtable has undergone a procurement which is currently in the process of being renewed.Airtable has has MFA available and users are managed by Peter Lewin and Andy Wood. The AM will be responsible for GDPR / data retention to be dealt with by assignment.
   b. No personal information will be held on Airtable.
6. We will require our Consortium Partners to operate on their Corporate IT issued by their parent organisation and use their Corporate Email accounts for communication. We will only share Assignment documentation with members of the Consortium using Corporate Email or through the Teams site.

Assessment of Risk

ISO27001 recommends that a risk assessment is completed to identify and help protect key assets associated with the assignment.

ASSET	
Asset Details What do you need to protect? (e.g. data, intellectual property)	Intellectual Property of design and strategies relating to the project. Data relating to scheduling, progress of reform implementation, learnings, insights from data analytics and communications sessions being delivered as part of the programme. This includes some corporate information which includes personal identifiers limited to Name, Email, Organisation, Role. This information will be

	mastered and managed in the AirTable platform. High level data relating to areas of interest for DfE SEND and AP programme e.g. Systems and Places – e.g. Location of implementation changes, reform information, Local authority types and sizes. This information will not include individual data on individuals. This information will be mastered and managed in the AirTable platform.
Owner Who is legally responsible for the asset above? (e.g. PiC, Client, Client's supplier)	PiC
Value What value does the asset have (e.g. a monetary value, or is it company intellectual property?)	Company Intellectual Property
Impact What would the consequences be for PA/the client if the asset were lost, stolen or disclosed to unauthorised individuals? E.g.: High: Critical reputational/financial impact: Would potentially stop PA doing business in an entire sector Medium: May temporarily lose good relationship with major client, but damage recoverable Low: May cause PA minor embarrassment	Medium: May temporarily lose good relationship with major client, but damage recoverable.

THREATS	
Vulnerabilities What properties does the asset have which could mean it is vulnerable (e.g. the data is not encrypted, there are no backup copies of the information, the information could be shared with people who do not have permission to see it, the asset is physically fragile etc)?	The information could be downloaded by partner companies and shared with someone who does not have permission to see it. Data is held in AirTable Platform with appropriate controls and protection.
Threat Rating Think about your answer to the 'Impact' section earlier in this form. How severe is the above vulnerability (e.g. High, Medium or Low)?	Low

Range / Environment How far reaching are the consequences of the asset being compromised? (e.g. Local, National, Global)	Only relevant to similar projects, but could be on a national level
Threats Considering the vulnerability listed above, are there any ways someone might exploit this to gain access/harm the asset (e.g. hacking, theft, acts of god, terrorism, unauthorised disclosure, breach of law)?	Unauthorised disclosure. The assignment team will be very careful with the material that they add to this shared site as there are partners who can access, so the threat is low.
Likelihood How likely is the above to happen?	Not likely
Mitigation How will PA work on the assignment to mitigate the risks above, or minimise them?	The assignment team will have a shared Teams site to keep all sensitive material and documents. All partner organisations will be briefed and contractually required to comply with this assignment security plan. The AirTable platform provided for different levels of access. Only the PA team will have editor rights. Partner and client organisations will only be able to access carefully controlled and limited views relevant to their requirements.

RISKS			
Risk If the above mitigations are observed, what is the risk of the above scenarios happening	Very Low risk		
Further mitigation Are there any additional actions that PA can complete to minimise risk to this asset?	Mark all materials with Confidential and PDF documents where possible		
Review Dates Set a date to regularly review this ASP to	01/10/2023	01/01/2024	

ensure that it is still applicable.			

Finally, include anything that you feel is relevant to the assignment but not covered above. Operational Risk is always happy to provide advice and guidance with your ASP.

6 agreement

Assignment Security Plans and H&S assessments **when required** should be shared ** between the Partner in Charge and the Client. This ensures that all parties have a firm understanding of the obligations and capabilities and agree to adopt the appropriate behaviours.

The measures highlighted in this security plan aim to mitigate the specific security risks identified in the assignment and are agreed between:

1. [redacted]

2. [redacted]

For the purposes of this agreement, it is agreed that the following roles and responsibilities will be adopted:

Roles and Responsibilities

		Contact Number

***** *In the spirit of collaboration and to set expectations at the outset of an assignment, it is advantageous to ensure the client is cognisant of the proposed assignment security mitigations. Indeed, in many cases the client may be able to assist in enhancing and developing the security measures in the plan. However, there may be assignments where we would not wish to share our detailed security methodology with the client, but rather to outline our approach more generally. The Partner in Charge must weigh the benefits of either approach before deciding whether to share the Assignment Security Plan or not. In all cases, the Partner in Charge must authorise the Assignment Security Plan.*

Once completed, please save a copy in the Teams site in Office 365 / approved system jobsite / commercial file and email a copy of this ASP to [redacted]. Operational Risk may require changes to content for the purposes of clarity.

7 Appendix A

ONLY REQUIRED WHERE PERSONAL DATA IS IDENTIFIED

7.1 DATA PRIVACY IMPACT ASSESSMENT (DPIA)

7.2 PA'S STANCE ON PERSONAL DATA PROCESSING

Occasionally, PA will need to process personal data on behalf of clients in order to deliver the agreed engagement. Unless otherwise stated in this agreement, PA will:

- avoid holding personal data on the PA network and process all personal data on the client's own systems
- where the above is not practicable, data held on the PA network will always be anonymised
- where anonymisation is not possible, PA will separate the personal data from all other PA data on the PA network so that it is subject to unique controls and can be deleted in its entirety at the end of the engagement.

If for any reason you are not able to comply with the above on this assignment, please contact [redacted] immediately for guidance.

7.3 DPIA QUESTIONNAIRE

SECTION ONE: ASSIGNMENT INFORMATION

Question	Response
What personal information will be collected as part of this assignment? (e.g. Name, DOB, Address, Political Views, Patient Health Information etc.)	
Who is the business owner of this information? (e.g. PA, client)	
What is the justification for collecting this information? (e.g. Does PA really need this information? Could we work with anonymised data instead?)	
Will we be working on this information using the client's IT systems, or PA IT systems?	
Who will require access to this information within PA?	
Will any third parties/contractors also require access to this information?	

SECTION TWO: INFORMATION FLOWS

Complete this section to describe how the personal information will flow throughout different phases/activities within the assignment:

CREATION OF INFORMATION	
How will the personal information be created/collected?	

ACCESS TO INFORMATION	
How will PA people access the information?	
What is the approval process for granting access/removing access to this information?	

TRANSFER OF INFORMATION	
How will the personal information be transferred between PA and the client?	

STORAGE OF INFORMATION	
How will the personal information be stored?	
Who will have access to it?	

HANDOVER / DESTRUCTION OF INFORMATION	
How will the personal information be handed over to the client or destroyed at the end of the assignment?	

SECTION THREE: CONSULTATION

Question	Response
What practical steps will you take to ensure that you identify and address privacy risks?	
Who will need to be consulted on the privacy risks, internally and externally (if anyone)?	

If applicable, how will this consultation be carried out?	

SECTION FOUR: PRIVACY RISKS AND MITIGATIONS

Complete the table below to list all privacy risks and how they will be mitigated:

Privacy Issue	Risk to individuals	Risk to PA/client organisation	Mitigation

Document Control information

REVIEW HISTORY

Document Information	
Status:	Final
Control ID:	[Control ID]
Document Type:	Risk Assessment
Reference:	[DocRefID]
Valid To:	[Valid To]
Owner:	[Owner]
Origin:	[Origin]
Approved by:	[Approved By]
Version:	V1

1. Schedule 16 (Buyer Specific Security Requirements)

2.

3. Definitions

4.

1. In this Schedule, the following words shall have the following meanings and they shall supplement the other definitions in the Contract:

5.

6. "BPSS" 7. "Baseline Personnel Security Standard"	8. the Government's HMG Baseline Personal Security Standard. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
9. "CCSC" 10. "Certified Cyber Security Consultancy"	11. is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. 12. See website: 13. https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
14. "CCP" 15. "Certified Professional" 16.	17. is a NCSC scheme in consultation with government, industry, and academia to address the growing need for specialists in the cyber security profession. See website: 18. https://www.ncsc.gov.uk/information/about-certified-professional-scheme
19. "Cyber Essentials" 20. "Cyber Essentials Plus"	21. Cyber Essentials is the government backed industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. 22. There are a number of certification bodies that can be approached for further advice on the scheme, the link below points to these providers: 23. https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body

24. "Data" 25. "Data Controller" 26. "Data Protection Officer" 27. "Data Processor" 28. "Personal Data" 29. "Personal Data requiring Sensitive 30. Processing" 31. "Data Subject", "Process" and "Processing"	32. shall have the meanings given to those terms by the Data Protection Legislation
33. "Buyer's Data" 34. "Buyer's Information"	35. is any data or information owned or retained to meet departmental business objectives and tasks, including: 36. (a) any data, text, drawings, diagrams, images, or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical, or tangible media, and which are: 37. (i) supplied to the Supplier by or on behalf of the Buyer; or 38. (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or 39. (b) any Personal Data for which the Buyer is the Data Controller;
40. "Departmental Security Requirements"	41. the Buyer's security policy or any standards, procedures, process, or specification for security that the Supplier is required to deliver.
42. "Digital Marketplace / G-Cloud"	43. the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
44. "End User Devices"	45. the personal computer or consumer devices that store or process information.
46. "Good Industry Standard" 47. "Industry Good Standard"	48. the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight, and timeliness as would be expected from a leading company within the relevant industry or business sector.
49. "GSC" 50. "GSCP" 51.	52. the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications

53. “HMG”	54. Her Majesty’s Government
55. “ICT”	56. Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
57. “ISO/IEC 27001” “ISO 27001”	58. is the International Standard for Information Security Management Systems Requirements
59. “ISO/IEC 27002” “ISO 27002”	60. is the International Standard describing the Code of Practice for Information Security Controls.
61. “ISO 22301”	62. is the International Standard describing for Business Continuity
63. “IT Security Health Check (ITSHC)” 64. “IT Health Check (ITHC)” 65. “Penetration Testing”	66. an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that ICT system.
67. “Need-to-Know”	68. the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.
69. “NCSC”	70. the National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
71. “OFFICIAL” 72. 73. 74. 75. “OFFICIAL-SENSITIVE”	76. the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP). 77. 78. the term ‘OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen, or published in the media, as described in the GSCP.
79. “RBAC” 80. “Role Based Access Control”	81. Role Based Access Control, a method of restricting a person’s or process’ access to information depending on the role or functions assigned to them.
82. “Storage Area Network” 83. “SAN”	84. an information storage system typically presenting block-based storage (i.e., disks or virtual disks) over a network interface rather than using physically connected storage.

85. “Secure Sanitisation” 86. 87.	88. the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. 89. 90. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media 91. 92. The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction-0
93. “Security and Information Risk Advisor” 94. “CCP SIRA” 95. “SIRA”	96. the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: 97. https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
98. “Senior Information Risk Owner” 99. “SIRO”	100. the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arm’s length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties. 101.
102. “SPF” 103. “HMG Security Policy Framework”	104. the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently, and securely. https://www.gov.uk/government/publications/security-policy-framework
105. "Supplier Staff"	106. all directors, officers, employees, agents, consultants, and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier’s obligations under the Contract. 107.

108.

109. **Operative Provisions**

13. The Supplier shall be aware of and comply with the relevant HMG security policy framework, NCSC guidelines and where applicable these Departmental Security Requirements which include but are not constrained to the following paragraphs.

110. Guidance note: providers on the HMG Digital Marketplace / G-Cloud that have demonstrated compliance, as part of their scheme application, to the relevant scheme’s security framework, such as the HMG Cloud Security Principles for the HMG Digital Marketplace / G-Cloud, may on presentation of suitable evidence of compliance be excused from compliance to similar clauses within the DfE Security Requirements detailed in this section.

14. Where the Supplier will provide products or Services or otherwise handle information at OFFICIAL for the Buyer, the requirements of Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 dated 25 May 2016, or any subsequent updated document, (PPN 09/23: Updates to the Cyber Essentials Scheme), are mandated, namely that "contractors supplying products or services to HMG shall have achieved, and will be expected to retain Cyber Essentials certification at the appropriate level for the duration of the contract". The certification scope shall be relevant to the Services supplied to, or on behalf of, the Buyer.

111. Guidance note: details of the acceptable forms of equivalence are stated at Section 9 of Annex A within https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification the link to Cabinet Office document in this paragraph).

112. Guidance note: the Buyer's expectation is that the certification scope will be relevant to the Services supplied to, or on behalf of, the Buyer. However, where the Supplier or (sub) contractor is able to evidence a valid exception or certification to an equivalent recognised scheme or standard, such as ISO 27001, then certification under the Cyber Essentials scheme could be waived. Changes to the Cabinet Office Action Note will be tracked by the DfE)

113. Guidance note: the Buyer's expectation is that SMEs or organisations of comparable size shall be expected to attain and maintain Cyber Essentials. Larger organisations or enterprises shall be expected to attain and maintain Cyber Essentials Plus.)

15. Where paragraph 1.2 above has not been met, the Supplier shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope relevant to the Services supplied to, or on behalf of, the Buyer. The scope of certification and the statement of applicability must be acceptable, following review, to the Buyer, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

114. Guidance note: the Buyer's expectation is that suppliers claiming certification to ISO/IEC 27001 shall provide the Buyer with copies of their Scope of Certification, Statement of Applicability and a valid ISO/IEC 27001 Certificate issued by an authorised certification body. Where the provider is able to provide a valid Cyber Essentials certification then certification under the ISO/IEC 27001 scheme could be waived and this paragraph may be removed.)

16. The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Buyer's Data being handled in the course of providing the Services and will handle all data in accordance with its security classification. (In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Buyer's Data).

115. Guidance note: the Buyer's expectations are that all contractors shall handle the Buyer's information in a manner compliant with the GSCP. Details of the GSCP

can be found on the GOV.UK website at: https://www.gov.uk/government/publications/government-security-classifications.)

116. Guidance note: compliance with the GSCP removes the requirement for the Buyer to issue a Security Aspects Letter (SAL) to the Supplier).

17. Buyer's Data being handled while providing an ICT solution or service must be separated from all other data on the Supplier's or sub-contractor's own IT equipment to protect the Buyer's Data and enable the data to be identified and securely deleted when required in line with paragraph 1.14. For information stored digitally, this must be at a minimum logically separated. Physical information (e.g., paper) must be physically separated.

117. Guidance note: advice on HMG secure sanitisation policy and approved methods are described at https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

18. The Supplier shall have in place and maintain physical security to premises and sensitive areas used in relation to the delivery of the products or Services, and that store or process Buyer's Data, in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g., door access), CCTV, alarm systems, etc.

118. Guidance note: where the Supplier's and sub-contractor services are wholly carried out within Buyer premises and all access to buildings or ICT systems is managed directly by the Buyer as part of the service, the Buyer shall be responsible for meeting the requirements of this paragraph.)

19. The Supplier shall have in place, implement, and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Buyer's Data. This policy should include appropriate segregation of duties and if applicable role-based access controls (RBAC). User credentials that give access to Buyer's Data or systems shall be considered to be sensitive data and must be protected accordingly.

119.

120. Guidance note: where the Supplier's and sub-contractor services are wholly carried out within Buyer premises and all access to buildings or ICT systems is managed directly by the Buyer as part of the service, the Buyer shall be responsible for meeting the requirements of this paragraph.)

20. The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer's Data, including but not limited to:

21. physical security controls;
22. good industry standard policies and processes;
23. malware protection;
24. boundary access controls including firewalls, application gateways, etc;
25. maintenance and use of fully supported software packages in accordance with vendor recommendations;
26. use of secure device configuration and builds;
27. software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;

28. user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;

29. any services provided to the Buyer must capture audit logs for security events in an electronic format at the application, service and system level to meet the Buyer's logging and auditing requirements, plus logs shall be:

30. retained and protected from tampering for a minimum period of six months;

31. made available to the Buyer on request.

121. Guidance note: where the Supplier's and sub-contractor services are wholly carried out using Buyer ICT resources or locations managed directly by the Buyer as part of the service, the Buyer shall be responsible for meeting the requirements of this paragraph.)

122.

123. Guidance note: The Minimum Cyber Security Standard issued by Cabinet Office and Information Commissioner's Office advice for the protection of sensitive and personal information recommends the use of Multi-Factor Authentication (MFA). The MFA implementation must have two factors as a minimum; with the second factor being facilitated through a separate and discrete channel, such as, a secure web page, voice call, text message or via a purpose-built mobile app, such as Microsoft Authenticator.)

124. Guidance note: Further advice on appropriate levels of security audit and log collection to be applied can be found at: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-1-security-monitoring.)

32. The Supplier shall ensure that any Buyer's Data (including email) transmitted over any public network (including the Internet, mobile networks, or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.

33. The Supplier shall ensure that any Buyer's 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 Buyer except where the Buyer has given its prior written consent to an alternative arrangement.

125. Guidance note: The use of an encryption product that utilises the AES 256 algorithm would be considered 'industry good practice' in this area. Where the use of removable media as described in this paragraph is either prohibited or not required in order to deliver the Services this paragraph shall be revised as follows: - 'The use of removable media in any form is not permitted'.)

34. The Supplier shall ensure that any device which is used to process Buyer's 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: https://www.ncsc.gov.uk/guidance/end-user-device-security and https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles.

126. Guidance note: The use of an encryption product that utilises the AES 256 algorithm would be considered 'industry good practice' in this area. Where the Supplier's and sub-contractor Services are wholly carried out using Buyer ICT

resources managed directly by the Buyer as part of the Services, the Buyer shall be responsible for meeting the requirements of this paragraph.)

1. Whilst in the Supplier's care all removable media and hardcopy paper documents containing Buyer's Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

127. The term 'lock and key' is defined as: "securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user's sole control and to which they hold the keys".

128. Guidance note: Further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at: https://www.cpni.gov.uk/secure-destruction-0)

When necessary to hand carry removable media and/or hardcopy paper documents containing Buyer's Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This paragraph shall apply equally regardless of whether the material is being carried inside or outside of company premises.

129. The term 'under cover' means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

1. In the event of termination of Contract due to expiry, as a result of an Insolvency Event or for breach by the Supplier, all information assets provided, created or resulting from provision of the Services shall not be considered as the Supplier's assets and must be returned to the Buyer and written assurance obtained from an appropriate officer of the Supplier that these assets regardless of location and format have been fully sanitised throughout the Supplier's organisation in line with paragraph 1.15.

130. Guidance note: it is Buyer policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning sanitisation must be in accordance with guidance provided by NCSC and CPNI.)

1. In the event of termination, equipment failure or obsolescence, all Buyer's Data and Buyer's Information, in either hardcopy or electronic format, that is physically held or logically stored by the Supplier must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC-approved product or method.

131. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Supplier shall protect (and ensure that any sub-contractor protects) the Buyer's Information and Buyer's Data until such time, which may be long after termination or expiry of the Contract, when it can be securely cleansed or destroyed.

132. Evidence of secure destruction will be required in all cases.

133. Guidance note: where there is no acceptable secure sanitisation method available for a piece of equipment, or it is not possible to sanitise the equipment due to an irrecoverable technical defect, the storage media involved shall be destroyed using an HMG approved method described at https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.)

134. Guidance note: further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at: https://www.cpni.gov.uk/secure-destruction-0)

135. Guidance note: the term ‘accounted for’ means that assets and documents retained, disposed of or destroyed should be listed and provided to the Buyer as proof of compliance to this paragraph.)

2. Access by Supplier Staff to Buyer’s Data, including user credentials, shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Buyer. All Supplier Staff must complete this process before access to Buyer’s Data is permitted. [Any Supplier Staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact].

136. Guidance note: further details of the requirements for HMG BPSS clearance are available on the website at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard)

137. Guidance note: further details of the requirements for National Security Vetting, if deemed necessary for this contract are available at: https://www.gov.uk/government/publications/hmg-personnel-security-controls)

138. Guidance note: the definition of “Supplier Staff” must include supplier subcontractors’ staff. Please ensure that “Supplier Staff” is included in the schedule definitions unless this same definition is included elsewhere such as is the case for the Mid-tier Contract and Short Form Contract.)

3. All Supplier Staff who handle Buyer’s Data shall have annual awareness training in protecting information.

139. Guidance note: the definition of “Supplier Staff” must include supplier subcontractors’ staff. Please ensure that “Supplier Staff” is included in the schedule definitions unless this same definition is included elsewhere such as is the case for the Mid-tier Contract and Short Form Contract.)

1. Notwithstanding any other provisions as to business continuity and disaster recovery in the Contract, the Supplier shall, as a minimum, have in place robust business continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the Contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency, or crisis to the Services delivered. If an ISO 22301 certificate is not available, the supplier will provide evidence of the effectiveness of their ISO 22301 conformant business continuity arrangements and processes

including IT disaster recovery plans and procedures. This must include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

140. Guidance note: the business continuity and disaster recovery plans should be aligned with 'industry good practice' and it is the Buyer's expectation that all vendors providing services or infrastructure to the Buyer will have plans that are aligned to the ISO 22301 standard in place. Further information on the requirements of ISO 22301 may be found in the standard.)

1. Any suspected or actual breach of the confidentiality, integrity, or availability of Buyer's Data, including user credentials, used or handled while providing the Services shall be recorded as a Security Incident. This includes any non-compliance with the Departmental Security Requirements and these provisions, or other security standards pertaining to the solution.

141. Security Incidents shall be reported to the Buyer immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If Security Incident reporting has been delayed by more than 24 hours, the Supplier should provide an explanation about the delay.

142. Security Incidents shall be reported through the Buyer's nominated system or service owner.

143. Security Incidents shall be investigated by the Supplier with outcomes being notified to the Buyer.

1. The Supplier shall ensure that any Supplier ICT systems and hosting environments that are used to handle, store or process Buyer's Data, including Supplier ICT connected to Supplier ICT systems used to handle, store or process Buyer's Data, shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the Services being provided are to be shared with the Buyer in full without modification or redaction and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required, to be determined by the Buyer upon review of the ITHC findings.

144.

145. Guidance note: further information on IT Health Checks and the NCSC CHECK Scheme which enables penetration testing by NCSC approved companies can be found on the NCSC website at: https://www.ncsc.gov.uk/scheme/penetration-testing.)

2. The Supplier or sub-contractors providing the Services will provide the Buyer with full details of any actual or future intent to develop, manage, support, process, or store Buyer's Data outside of the UK mainland. The Supplier or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.

146. Guidance note: the offshoring of HMG information outside of the UK is subject to approval by the Buyer's SIRO.)

3. The Buyer reserves the right to audit the Supplier or sub-contractors providing the Services within a mutually agreed timeframe

but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the Services being supplied and the Supplier's, and any sub-contractors', compliance with the paragraphs contained in this Schedule.

4. The Supplier and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the Buyer. This will include obtaining any necessary professional security resources required to support the Supplier's and sub-contractor's security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.

147. Guidance note: it is the Buyer's policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning their organisation. Further advice and guidance on the Buyer's security assurance processes can be supplied on request. Information about the HMG Supplier Assurance Framework can be found at: https://www.gov.uk/government/publications/government-supplier-assurance-framework)

148. Guidance note: further information on the CCP and CCSC roles described above can be found on the NCSC website at: https://www.ncsc.gov.uk/information/about-certified-professional-scheme and https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy)

5. Where the Supplier is delivering an ICT solution to the Buyer they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Buyer's Policy. The Supplier will provide the Buyer with evidence of compliance for the solutions and services to be delivered. The Buyer's expectation is that the Supplier shall provide written evidence of:

6. compliance with HMG Minimum Cyber Security Standard.

7. any existing security assurance for the Services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification (e.g., United Kingdom Accreditation Service).

8. any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.

1. documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Supplier shall provide details of who the awarding body or organisation will be, and date expected.

149. Additional information and evidence to that listed above may be required to ensure compliance with DfE security requirements as part of the DfE security assurance process. Where a request for evidence or information is made by the Buyer, the Supplier will acknowledge the request within 5 working days and either provide the information within that timeframe, or, if that is not possible, provide a date when the

information will be provided to the Buyer. In any case, the Supplier must respond to information requests from the Buyer needed to support the security assurance process promptly and without undue delay.

2. The Supplier shall contractually enforce all these Departmental Security Requirements onto any third-party suppliers, sub-contractors or partners who could potentially access Buyer's Data in the course of providing the Services.

3. The Supplier shall comply with the NCSC's social media guidance: how to use social media safely for any web and social media-based communications. In addition, any Communications Plan deliverable must include a risk assessment relating to the use of web and social media channels for the programme, including controls and mitigations to be applied and how the NCSC social media guidance will be complied with. The Supplier shall implement the necessary controls and mitigations within the plan and regularly review and update the risk assessment throughout the contract period. The Buyer shall have the right to review the risks within the plan and approve the controls and mitigations to be implemented, including requiring the Supplier to implement any additional reasonable controls to ensure risks are managed within the Buyer's risk appetite.

4. Any Supplier ICT system used to handle, store, or process the Buyer's Data, including any Supplier ICT systems connected to systems that handle, store, or process the Buyer's Data, must have in place protective monitoring at a level that is commensurate with the security risks posed to those systems and the data held. The Supplier shall provide evidence to the Buyer upon request of the protective monitoring arrangements in place needed to assess compliance with this requirement.