OFFICIAL

PSN CONNECTIVITY

APPENDIX 6

SECURITY PLAN

The Contractor shall ensure that its Security Plan reflects the Contractor's Response to the ITT in respect of security as the same are reproduced below.

A glossary of terms and abbreviations can be found at Annex 1-2 of Attachment 15.1.

References

Reference	Description
[1]	Cabinet Office Security Policy Framework https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf
[2]	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf
[3]	HMG Information Assurance Standard No 1 and 2 Technical Risk Management, Issue 4.0, April 2012
[4]	HMG Information Assurance Standard No 1 and 2 - Supplement Technical Risk Assessment, Issue 1.0 April 2012
[5]	CAS (T) – Audit Handbook for CESG Assured Service (Telecoms) (gpg32)

Contents

1. INTRODUCTION

1.1 This document, referred to hereafter as 'the Security Plan,' provides a high-level plain-English description of the information security responsibilities of the Contractor staff, sub-contractors and personnel involved in the Services options, to protect the security of any resulting customer information to which the Contractor has custody.

1.2 To that end, the Security Plan is made available to all members of staff, contractors and 3rd party personnel who sell, design, implement, manage, maintain the Service.

1.3 This document does not replace or supplant any other Contractor policy but offers specific, additional advice where necessary on particular security aspects relating to the Service, and guidance and links to where additional information may be found, with the aim of ensuring that The Contractor complies with its contractual requirements set out in Schedule 2.2 – Security Requirements and Plan, along with requirements defined in Annex 1 – Baseline Security Requirements. Where additional requirements are defined in Annex 2 – Service requirements – Security, the Contractor will review and confirm compliance as appropriate.

1.4 The scope of the Security Plan is specifically aimed to protect all elements associated with the delivery of the Service including premises, Contractor systems, any ICT and information and data traffic.

1.5 Information is structured in line with requirements of ISO27001 and IOS27002 and is cross-referenced with these standards as necessary.

1.6 The Contractor's already PSN certified Assured and Protect IP VPN service infrastructures are heavily referenced within this security plan as that infrastructure provides the foundation for connectivity of the Service.

1.7 Within 40 Working Days of the effective date of the framework agreement a fully complete and up-to date security plan will be provided to the Customer Authority and any subsequent amendments and updates to the security plan will be completed within 10 Working Days after review with the Customer Authority.

2. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

2.1 The Contractor has an existing ISMS structure in line with sections 4.0, 5.0 and 6.0 of the ISO27001 standard which has been assessed using the CAS (T) certification

scheme which utilises all of the controls defined within ISO270001 complemented with others from ISO270011.

2.2 The Contractor does not have ISO27001 certification for the Service being proposed to the Customer Authority, however can confirm that it has attained CAS (T) certification and PSN accreditation for its PSN IPVPN Service and complies with the objectives of ISO27001. In addition the contractor has gained PGA certification for its PSN encrypted (protect) service which forms the foundation of its PSN IPED service offering.

2.3 The Contractor is committed to ensure that its ISMS is developed, certified, maintained and improved, and the Service associated with this security plan will fall within the scope of this ISMS.

2.4 The Contractor is committed to ensure that the ISMS complies with the Security Policy Framework obligations and Baseline Security Requirements for the purposes of ensuring that all accreditation and secure connectivity objectives are achieved.

2.5 The Contractor undertakes to consider suggested improvements and effectiveness of the ISMS by the Customer Authority, including measures to identify effectiveness of controls.

2.6 The Scope of the ISMS will be adjusted to include new services as and when they become applicable to the Customer Authority and the following aspects will be included within the scope of the ISMS:

- equipment on the Customer Authority premises managed by the Contractor or their authorised agents
- equipment held on the Contractor's (or their authorised agents) network that are critical to the provision of the Service i.e. without these the end customer cannot access the Service.
- the management systems on Contractor (or their authorised agency) premises that configure or have access to the equipment being managed.
- the Contractor's (or their authorised agency) premises in which the management systems or critical network equipment are located.
- personnel or groups of personnel who have the ability to directly reconfigure the equipment.

- other business activities carried out by the Contractor such as HR activities, Business Continuity, and Change Management which require processes and procedures are covered by generic compliance with the requirements of the CAS (T) certification scheme.
- the Contractor will perform annual penetration testing for individual services and maintain a risk register/remediation log for the purposes of tracking and managing to resolution vulnerability issues identified during an ITHC/penetration test or for the management and acceptance of risk.

2.7 The following aspects are OUTSIDE the scope of the ISMS:

- the Customer Authority premises including environmental systems
- business support systems at the Contractor's (or their authorised agency) premises that do not have direct access to the equipment being managed e.g. billing, invoicing and order management systems.

3. SECURITY TESTING

3.1 The Contractor approach to security testing complies with the requirements of ISO27001 to carry out annual ITHC/penetration tests. Services that carry certification have ITHC/penetration tests carried out by CESG approved CHECK Green certified companies with the scope of testing conforming to the accredited scope of the service. Additionally from time to time services may be subject to internal penetration testing to identify vulnerabilities associated with aspects of a particular service.

3.2 The Contractor completes CAS (T) certification of its services where accreditation of PSN connectivity services is required. Where self-assertion of services for PSN is required then the Contractor will conform to the developing standards for this activity.

3.3 The Contractor reviews the scope of its ISMS, led by the Contractor's chief security officer, at least annually and all aspects of the operation of the ISMS is reviewed to determine fitness for purpose and The Contractor commits to act on the recommendations produced by the review.

3.4 Where the Customer Authority wishes to carry out their own audit or assessment of the Contractor's ISMS or perform an ITHC in addition to the assessments carried out as part of the CAS (T) scheme requirements the Contractor will cooperate with these requirements as defined in Annex 2 – Service Requirements – Security and Baseline Security Requirements.

3.5 The resulting output from CAS (T) assessments and other audits which directly affect the vulnerability or performance of the Service significantly the Contractor will notify the Customer Authority of the issue and the action being taken to resolve the issue.

3.6 The Contractor commits to maintaining monitoring of the service via its security alarm monitoring system, which will proactively monitor the Service via log data for the purposes of generating security alarm signatures which will capture security threats and vulnerabilities. The output from the system provides one of the key mechanisms for the identification of a security breach incident, and should such an incident occur then the resulting information will potentially initiate the security incident process discussed in section 9.0 of this document.

4. SECURITY ASPECTS LETTER

4.1 The Contractor will use the security aspects letter (SAL) for the Service issued by the Customer Authority prior to the Effective Date to inform this Security Plan. The SAL provides authoritative statements about how the customer values specific information assets associated with the Service and delivers key messages that the Contractor and any sub-contractors must do to ensure their working arrangements do not compromise the confidentiality, integrity or availability of these information assets.

4.2 The Contractor shall assign a business classification of OFFICIAL for the Service being provided and where specific information is classified as OFFICIAL-SENSITIVE then additional measures (generally procedural or personnel) will be provided to reinforce the 'need to know' to safeguard that information. Also where there is a clear and justifiable requirement to reinforce the 'need to know' assets will be marked OFFICIAL-SENSITIVE.

4.3 Where the Contractor is found not to conform to the Service classification of OFFICIAL this will be subject to a change control notice.

4.4 Relevant parts of any RMADS produced and maintained by the Contractor during the life of the service shall reflect the specific demands of the SAL.

5. SECURITY INFORMATION DISSEMINATION

5.1 The contents of the Customer Authority SAL will be published on the Contractor's intranet along with guidance on interpretation.

5.2 The Contractor's global security organisation, supported by senior management, shall ensure that all staff and contractors concerned with the service will be provided with a security briefing on the security aspects of the Service, within 60 Working Days of the Effective Date of the Service framework being agreed.

5.3 The security briefing will cover a minimum of :

- location of key security document
- any security aspects which are not 'business-as-usual
- security roles (accreditor, sponsor etc.)
- where to find additional guidance, e.g. ISMS/hub documents and CESG guidance.

6. ACCREDITATION

6.1 The underlying IP VPN service has been accredited, being aligned to reference **5,** and where agreed with the Customer Authority if supplementary audit/accreditation is required for the Service then this will have been completed or within 90 Working Days of the effective date of the contract.

6.2 The Contractor employs a security team for the purpose of assisting in this accreditation.

6.3 The Contractor has chosen to supplement the security team by turning to specialist members of the CESG listed adviser scheme (CLAS) and service providers approved under the CHECK scheme when such needs arise, for example as part of the annual IT health check.

6.4 The security measures to be implemented and maintained by the Contractor in relation to all aspects of the Service will be documented in a risk management and accreditation document set (RMADS) or a replacement vehicle should the RMADS process become superseded.

6.5 The Security controls adopted will be proportionate to manage the risks. The Contractor will conform to the requirements of reference **5**. Any non-conformities will be noted in a residual risk statement for the service.

6.6 RMADS provide a structure which is used to assemble portfolios of documents that will collectively:

- explain the business purpose and scope;

  summarise the key computer systems, networks, services and locations;

- identify and quantify risks that may damage the integrity, availability or confidentiality of information dealt with by these computer systems, networks and services;
- describe the blend of physical, personnel, procedural and technical security controls used to manage these risks;
- provide regular evidence, such as security test, security inspection and security incident reports, to demonstrate that the security controls used manage these risks work effectively in practice.

6.7 References **3** and **4** are used as a basis for the risk assessment used within the RMADS. Reference **3** provides HMG's technical risk assessment method – a systematic approach to documenting and quantifying technical risks that may threaten the integrity, availability or confidentiality of a computer system, network or service. Reference **4** provides HMG's technical risk treatment method – a structured approach to documenting a security case that describes the nature and stringency of the security controls and assurances needed to manage any risks identified by applying the method in reference **3.**

6.8 Where the use of references **3** and **4** are no longer deemed appropriate then The Contractor commits to conform to the latest guidance being produced by CESG on the management of risk.

6.9 When assessing risk treatment, the Contractor will use a risk tolerance level specified by the Customer Authority before the Effective Date to inform this Security Plan. The risk tolerance level shall specify the level of risk that the Customer Authority is prepared to accept. If the risk tolerance level is not agreed prior to the Effective Date of the Service then a risk tolerance of 'medium' will be adopted. Any change to the risk tolerance level after the Effective Date is deemed a change to the Agreement.

6.10 Where aspects of the Service within the accreditation or ISMS scope are held offshore the customer will be advised within the service residual risk statement.

6.11 A privacy impact assessment will be undertaken by the Contractor's global security organisation and included in the RMADS.

6.12 The RMADS will be included within the ISMS structure, be available to appropriately-cleared personnel and be held and maintained by the Contractor and be available for inspection.

6.13 The RMADS will be structured according to ISO27001, cross-referencing if necessary to schedules within the Service and reference **1.**

7. TRANSITION

7.1 Where the Service is not currently part of the ISMS, the Contractor's global security organisation will be responsible, using reasonable endeavours and due process, for transition of the security arrangements and responsibilities for the Service into the scope of the ISMS within 60 Working Days of the Effective Date of the Service and highlight any outstanding residual risks associated with the service.

7.2 Notwithstanding this, where existing policies, procedures and work instructions already within the scope of the ISMS may be applied to the Service these will be included within the service scope as the service is developed and prior to production.

7.3 It is assumed that where sponsorship is required from the Customer Authority to gain PGA or similar support that this will be granted in a timely manner.

8. PERSONAL SECURITY

8.1 All Contractor employees, their agents and sub-contractors shall undertake to be part of The Contractor's EMEA security vetting process or equivalent for staff located overseas.

8.2 All EMEA staff of the Contractor that is associated either directly or indirectly with delivery, configuration and maintenance of OFFICIAL **2** services are subject to security vetting carried out to baseline personnel security standard (BPSS).

8.3 BPSS vetting is initiated by the Contractor's HR department and requires that the following checks are carried out:

- identity check
- confirmation of nationality and immigration status
- employment history (for the past 3 years)
- third–party verification of unspent convictions.

8.4 Some operational positions are security vetted to Security Clearance (SC) and where additional positions that are agreed to require additional vetting to SC that relate directly to the Customer Authority service then it will be expected that the Customer Authority will provide sponsorship to carry out this additional vetting, this includes staff physically attending customer premises.

8.5 All staff employed by the Contractor are required as part of the personal vetting procedure to acknowledge compliance with the security policies and standards of the

Contractor and are required to undertake mandatory annual security awareness training, this is compulsory for all employees.

9. SECURITY INCIDENT REPORTING

9.1 Where any specific security threats or security breaches are identified then the Contractor undertakes to report the incidents in a timely manner to the Customer Authority, immediately as possible in the event of a high risk issue. In addition where any specific security threats or security breaches identified by the Customer Authority are to be notified to the Contractor then the contact point will be the global security organisation via the Contractor's customer services manager or nominated security manager within the Contractor's company.

9.2 All security breaches identified by the Contractor are subject to a defined process and procedures with escalation up to and including the Contractor's chief security officer where warranted. Initial security breach investigations are processed by trained and experienced security NOC personnel who will analyse and prioritise the incident in-line with proven processes.

9.3 The Contractor will commit to security investigators being assigned to an incident depending on severity and within the process escalation triggers, escalation call lists, and time thresholds are included. Additional process features where a security breach plan has been activated include the following:

- activation/mobilisation plan
- communications plan
- event command and control process
- post event review

9.4 Where breaches of security materially affect the terms of a certified service then the certification body will also be notified and an assessment can then be carried out to determine whether a supplementary audit is required.

10. VULNERABILITIES OR MALWARE

10.1 It is not expected that The contractor will be in position to introduce any vulnerabilities, malware or virus infected files into the Customer Authority ICT environment as the Contractor has adopted multiple layers of anti-virus software within its corporate and service architecture and has deployed software to detect and

delete malware from within its service and related corporate and management environments.

10.2 However if malware is found the Contractor will cooperate with the Customer Authority to reduce and manage the effects of malware and limit any loss in operational efficiency of the Service.

11. RESPONSIBILITIES OF THE CONTRACTOR

11.1 The Contractor shall maintain accreditation for the Service and provide a copy of the accreditation statement upon request.

11.2 The Contractor shall provide a service residual risk statement. This shall provide the Customer Authority with summary details of the main residual risks and non-conformities, together with risk management statement and guidance on SyOPs that should be adopted by a customer's staff to operate the service securely.

11.3 The Contractor will complete annual penetration testing for the Service.

11.4 The Contractor shall maintain the Service in line with emerging changes in good industry practice.

11.5 Accommodate audit requirements of the Customer Authority.

11.6 Ensure that any 3rd party employed for the purposes of supporting the Service are aligned with the security policies and standards defined by the Contractor.

12. RESPONSIBILITIES OF THE CUSTOMER AUTHORITY

12.1 The Customer Authority shall provide their risk tolerance level to the Contractor.

12.2 The Customer Authority will provide a completed SAL to the Contractor.

12.3 The Customer Authority shall undertake a privacy impact assessment for the Service and provide it to The Contractor.

12.4 The Customer Authority shall provide the contact details of their security contact point for the reporting of security incidents.

13. AMENDMENT AND REVISION OF THIS PLAN

13.1 The Security Plan shall be reviewed annually from the Effective Date by the Contractor's global security organisation and the Customer Authority representative to ensure that it complies with current CESG good practice guidance, amendments in

GDS/PSN compliance process, amendments to systems, processes and any development of the related services.

13.2 Where inconsistencies between this security plan and the delivered service are found, either conformance with hardware requirements or standards and policies, then the Customer Authority will be notified within 3 Working Days by The Contractor and await feedback to identify if this plan requires amendment and re-issue.

OFFICIAL

CONTRACTOR'S RESPONSE TO THE ITT IN RESPECT OF THE SECURITY PLAN

Section 4: Security

Question 1: Security Management Plan

Criterion Weight	**60%**	**Criterion Tier 3**	**Security Management Plan**
Question 1		Contractors should set out by way of narrative and where appropriate diagrams their draft security management plan	
Response Guidance Notes		The plan should meet the minimum security requirements of the Customer Authority as identified in the Service Requirements. This plan will be inserted into Appendix 6 of the Call-Off Form and will form part of the contract. Contractors should be aware that Schedule 2.2 of the Call-Off Terms has been amended and is set out in Appendix 15 of the Call-Off Form. Responses to be contained within a max of 15 pages of A4 (including any diagrams and appendices)	
Contractor Response ***The CPS claims an exemption from publishing this information under Section 43(1) of the FOI Act 2000***			

Section 4: Security

Question 2: Management of Security Breaches

Criterion Weight	**40%**	**Criterion Tier 3**	**Management of Security Breaches**
Question 2		Please explain how you would ensure that appropriate processes were in place for this Contract for the handling of security breaches and how corrective actions will be approached and implemented and how this can be	

	proactively undertaken. Please advise where this links to the draft security plan submitted in relation to Question 1 of this Section 4
Response Guidance Notes	Set out by way of narrative and where appropriate diagrams, your draft processes and work instructions related to handling breaches in security, and how corrective actions will be approached and implemented where vulnerabilities are discovered Responses to be contained within a max of 15 pages of A4 (including any diagrams and appendices)
Contractor Response ***The CPS claims an exemption from publishing this information under Section 43(1) of the FOI Act 2000***	