Annex N: OFFICIAL and OFFICIAL- SENSITIVE Security Condition for UK Contracts

Definitions

1. The term *"Authority"* for the purposes of the Annex means a Ministry of Defence (MOD) official acting on behalf of the Secretary of State for Defence.

Security Grading

2. All aspects associated with this Contract are classified OFFICIAL. Some aspects are more sensitive and are classified as OFFICIAL-SENSITIVE. The Security Aspects Letter, issued by the Authority defines the OFFICIAL-SENSITIVE information that is furnished to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all OFFICIAL-SENSITIVE documents which it originates or copies during the Contract clearly with the OFFICIAL-SENSITIVE classification. However, the Contractor is not required to mark information/material related to the contract which is only OFFICIAL.

Official Secrets Acts

3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911-1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract (including sub-contractors) have notice that these statutory provisions, or any others provided by the Authority, apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

Protection of OFFICIAL and OFFICIAL- SENSITIVE Information

4. The Contractor shall protect OFFICIAL and OFFICIAL-SENSITIVE information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

5. The contractor shall apply Industry Security Notice (ISN) 2017/01 requirements to every industry owned IT and communication system used to store, process or generate MOD information including those systems containing OFFICIAL and/or OFFICIAL-SENSITIVE information. ISN 2017/01 details Defence Assurance and Risk Tool (DART) registration, IT security accreditation processes, risk assessment and risk management requirements. The ISN is available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/594320/DART_ISN_-_V2_3.pdf

6. OFFICIAL and OFFICIAL-SENSITIVE information shall be protected in a manner to avoid unauthorised access. The Contractor shall take all reasonable steps to prevent the loss, compromise or inappropriate access of the information or from deliberate or opportunist attack.

7. All OFFICIAL and OFFICIAL-SENSITIVE material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use OFFICIAL and OFFICIAL- SENSITIVE documents/material shall be handled with care. As a minimum, when not in use, OFFICIAL-SENSITIVE material shall be stored under lock and key and in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security and control.

8. Disclosure of OFFICIAL and OFFICIAL-SENSITIVE information shall be strictly in accordance with the *"need to know"* principle. Except with the written consent of the Authority, the Contractor shall not disclose any of the classified aspects of the Contract detailed in the Security Aspects Letter other than to a person directly employed by the Contractor or sub-Contractor, or Service Provider.

9. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 32.

Access

10. Access to OFFICIAL and OFFICIAL-SENSITIVE information shall be confined to those individuals who have a *"need-to-know"*, have been made aware of the requirement to protect the information and whose access is essential for the purpose of his or her duties.

11. The Contractor shall ensure that all individuals having access to OFFICIAL-SENSITIVE information have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to OFFICIAL-SENSITIVE information. Further details and the full requirements of the BPSS can be found at the Gov.UK website at:
https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.

Hard Copy Distribution

12. OFFICIAL and OFFICIAL-SENSITIVE documents shall be distributed, both within and outside company premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or Commercial Couriers in a single envelope. The words OFFICIAL or OFFICIAL-SENSITIVE shall not appear on the envelope. The envelope should bear a stamp or details that clearly indicates the full address of the office from which it was sent.

13. Advice on the distribution of OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of OFFICIAL-SENSITIVE hardware shall be sought from the Authority.

Electronic Communication, Telephony and Facsimile Services

14. OFFICIAL information may be emailed unencrypted over the internet. OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a CESG Commercial Product Assurance (CPA) cryptographic product or a MOD approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have TLS enabled. Details of the required TLS implementation are available at:

https://www.ncsc.gov.uk/guidance/tls-external-facing-services

Details of the CPA scheme are available at:

https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

Exceptionally, in urgent cases, OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so and only with the prior approval of the Authority.

15. OFFICIAL-SENSITIVE information shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the authority shall require. Such limitations, including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.

16. OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the UK and overseas. OFFICIAL-SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not within earshot of unauthorised persons.

17. OFFICIAL information may be faxed to recipients located both within the UK and overseas, however OFFICIAL-SENSITIVE information may be faxed only to UK recipients.

Use of Information Systems

18. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

19. The contractor shall ensure 10 Steps to Cyber Security is applied in a proportionate manner for each IT and communications system storing, processing or generating MOD UK OFFICIAL or OFFICIAL-SENSITIVE information. 10 Steps to Cyber Security is available at:

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

The contractor shall ensure competent personnel apply 10 Steps to Cyber Security.

20. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

21. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing OFFICIAL-SENSITIVE information on IT systems.

a. **Access Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of *"least privilege"* will be applied to System Administrators. Users of the IT System -Administrators should not conduct *'standard'* User functions using their privileged accounts.**

b. **Identification and Authentication (ID&A). All systems shall have the following functionality:**

(1) **Up-to-date lists of authorised users.**

(2) **Positive identification of all users at the start of each processing session.**

c. **Passwords. Passwords are part of most ID&A, Security Measures. Passwords shall be 'strong' using an appropriate method to achieve this, for example including numeric and *"special"* characters (if permitted by the system) as well as alphabetic characters.**

d. **Internal Access Control. All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.**

e. **Data Transmission. Unless the Authority authorises otherwise, OFFICIAL-SENSITIVE information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 13 above.**

f. **Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.**

(1). **The following events shall always be recorded:**

(a) **All log on attempts whether successful or failed,**

(b) **Log off (including time out where applicable),**

(c) **The creation, deletion or alteration of access rights and privileges,**

(d) **The creation, deletion or alteration of passwords,**

(2) **For each of the events listed above, the following information is to be recorded:**

(e) **Type of event,**

(f) **User ID,**

(g) **Date & Time,**

g. **Device ID, The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall**

also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know. If the operating system is unable to provide this then the equipment shall be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

h. **Integrity & Availability. The following supporting measures shall be implemented:**

(1). **Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruse power supply variations),**

(2). **Defined Business Contingency Plan,**

(3). **Data backup with local storage,**

(4). **Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software),**

(5). **Operating systems, applications and firmware should be supported,**

(6). **Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented,**

i. **Logon Banners Wherever possible, a *"Logon Banner"* shall be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text (depending on national legal requirements) could be:**

"Unauthorised access to this computer system may constitute a criminal offence"

j. **Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.**

k. **Internet Connections. Computer systems shall not be connected direct to the Internet or 'untrusted' systems unless protected by a firewall (a software based personal firewall is the minimum but risk assessment and management must be used to identify whether this is sufficient).**

l. **Disposal Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.**

Laptops

22. Laptops holding any MOD supplied or contractor generated OFFICIAL-SENSITIVE information are to be encrypted using a CPA product or equivalent as described in paragraph 14 above.

23. Unencrypted laptops not on a secure site[1] are to be recalled and only used or stored in an appropriately secure location until further notice or until

[1] Secure Sites are defined as either Government premises or a secured office on the contractor premises

approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt the term *"drives"* includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media e.g. CDs and DVDs), floppy discs and external hard drives.

24. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

25. Portable CIS devices are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss and Incident Reporting

26. The contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIAL-SENSITIVE information to the Authority.

27. Accordingly, in accordance with Industry Security Notice 2014/02 as may be subsequently updated at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/293480/ISN2014_02_Incident_Reporting.pdf

any security incident involving any MOD owned, processed, or Contractor generated OFFICIAL or OFFICIAL-SENSITIVE information defined in the contract Security Aspects Letter shall be immediately reported to the MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC). This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the MOD's Chief Information Officer (CIO) and, as appropriate, the company concerned. The MOD WARP will also advise the contractor what further action is required to be undertaken.

JSyCC WARP Contact Details
Email: For those with access to the RLI: CIO-DSAS-JSyCCOperations
Email: For those without access to the RLI: CIO-DSAS-JSyCCOperations@mod.gov.uk
Telephone: Working Hours: 0306 770 2187
Out of Hours/Duty Officer Phone: 07768 558863
Fax: 01480 446328
Mail: Joint Security Co-ordination Centre (JSyCC), X007 Bazalgette Pavilion, RAF Wyton, Huntingdon, Cambs, PE28 2EA.

Sub-Contracts

28. The Contractor may Sub-contract any elements of this Contract to Sub-contractors within the United Kingdom notifying the Authority. When sub-contracting to a Sub-contractor located in the UK the Contractor shall ensure that these Security Conditions shall be incorporated within the Sub-contract document. The prior approval of the Authority shall be obtained should the Contractor wish to Sub-contract any OFFICIALSENSITIVE elements of the Contract to a Sub-contractor located in another country. The first page of Appendix 5 (MOD Form 1686 (F1686)) of the Security Policy Framework Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at Appendix 5 at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367494/Contractual_Process_-_Appendix_5_form.doc.

If the Sub-contract is approved, the Contractor shall incorporate these security conditions within the Sub-contract document.

Publicity Material

29. Contractors wishing to release any publicity material or display hardware that arises from this contract shall seek the prior approval of the Authority. Publicity material includes open publication in the contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the MOD, Services or any other government department.

Private Venture

30. Any defence related Private Venture derived from the activities of this Contract are to be formally assessed by the Authority for determination of its appropriate classification. Contractors are to submit a definitive product specification for PV Security Grading in accordance with the requirement detailed at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414857/20150310_PV_Ex_Guidance_Document.pdf

Promotions and Potential Export Sales

31. Contractors wishing to promote, demonstrate, sell or export any material that may lead to the release of information or equipment classified OFFICIAL-SENSITIVE (including classified tactics, training or doctrine related to an OFFICIAL-SENSITIVE equipment) are to obtain the prior approval of the Authority utilising the MOD Form 680 process, as identified at:

https://www.gov.uk/mod-f680-applications.

Destruction

32. As soon as no longer required, OFFICIAL and OFFICIAL-SENSITIVE information/material shall be destroyed in such a way as to make reconstitution unlikely, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

33. Advice regarding the interpretation of the above requirements should be sought from the Authority.

34. Further requirements, advice and guidance for the protection of MOD information at the level of OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

https://www.gov.uk/government/publications/industry-security-notices-isns

Audit

35. Where considered necessary by the Authority, the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractors processes and facilities by representatives of the Authority to ensure compliance with these requirements.