PROTECTION OF AWE INFORMATION CLASSIFIED AT OFFICIAL & OFFICIAL-SENSITIVE

Contents

Introduction

1. With effect from 1st April 2015, AWE will adopt the Government Security Classification (GSC) system and introduce a new way of classifying information. GSC replaced the Government Protective Marking Scheme (GPMS) across most Government Departments in 2014.

2. Under GSC there are only three classifications: **TOP SECRET**, **SECRET** and **OFFICIAL**. Some information classified at OFFICIAL may attract additional handling constraints because of the sensitivity of that information and will be marked as **OFFICIAL-SENSITIVE** (effectively becoming a tier within the classification of OFFICIAL).

3. The use of the GPMS markings of RESTRICTED, PROTECT and UNCLASSIFIED will be discontinued, except in cases where there is a specific reason to retain the old markings authorised by MoD

4. Contractors who handle levels of information/material higher than OFFICIAL-SENSITIVE under the auspices of 'List X' will receive separate guidance covering those higher levels.

Purpose of Document

5. This document sets out AWE's requirements in order to ensure that information classified at OFFICIAL is effectively protected and handled appropriately when it is shared with AWE's contractors. It also provides guidance to AWE projects when engaging with current and/or prospective contractors; and to contractors and their sub-contractors in making appropriate arrangement to protect AWE's information. It also provides guidance for operating Third Party IT systems on an AWE site; on transmitting AWE's information offsite between AWE and its contractors; and on how contractors should transmit AWE's information between themselves and any sub-contractors.

Definitions

6. The term "AWE's information'' means any AWE or MoD information, whether protectively marked/classified or not, in any form, oral or recorded, which is released to a contractor by AWE, either directly or indirectly.

7. The term "AWE Security Authority" means the AWE List X Security Advisor (or their delegated representative).

8. The terms "Supply Chain", "Contractor/Supplier/Service Provider'' means any Third Party under contract to supply goods and/or services to AWE; or any Third Party that is a prospective supplier of goods and/or services to AWE.

9. The term "Sub-Contractor" means any Third Party which is under sub-contract to any AWE contractor for the provision of supporting goods and/or services to that contractor in respect of an AWE contract.

Release and Distribution

10. This is an OFFICIAL document, releasable to AWE contractors, prospective contractors and to sub-contractors. It may not be passed to any other Third Party who is not engaged in work for AWE without the express permission of the AWE Security Authority.

Applicability

11. The following security conditions apply to AWE information bearing a classification of **OFFICIAL** (and which includes **Reportable OFFICIAL** and **OFFICIAL-SENSITIVE)**.

GSC Guidance

12. Security classification arrangements under GSC are part of Her Majesty's Government's Security Policy Framework (SPF). More guidance on the SPF, GSC and associated material is available at:

https://www.gov.uk/government/collections/government-security#government-security-classifications

13. Guidance on the application of classifications in relation to AWE specific information should be sought from the relevant AWE Classification Officer if more detailed advice is required.

14. This document should be read in conjunction with the following documents (these will be enclosed where applicable):

    a. DEFCON 531: Disclosure of Information. All AWE contracts are subject to DEFCON 531 which requires the contractor to safeguard information provided by AWE and requires them to make sure that their employees are aware of their arrangements for so doing before they receive any information. There is a mutual obligation to treat in confidence all information disclosed in connection with or under the contract. DEFCON 531 covers all information primarily for protection of commercial interests by introducing a mutual obligation of confidentiality.

    b. DEFCON 76: Contractor's Personnel at Government Establishments. DEFCON 76 is included in all contracts where work is performed by contractors at AWE establishments. DEFCON 76 obligates the contractors' employees to comply with any regulations and rules in force whilst at AWE as required and dictated by the AWE Security Authority or their delegated representative.

    c. DEFCON 660: Reportable OFFICIAL[1]/OFFICIAL-SENSITIVE Security Requirements. This DEFCON is not yet agreed with Industry.

    d. Official Secrets Acts 1911-1989. The Official Secrets Acts protect any AWE information that may be received or generate, (irrespective of whether or not a contract or order is eventually placed). This includes any sketch, plan, model, article, note or document, or information connected with or arising out of AWE information. In addition, AWE premises are, and contractor premises are/will be Prohibited Places under the provisions of the Acts, and any AWE information is therefore information which relates to or is used in a Prohibited Place. The contractor shall take all

[1] **Reportable OFFICIAL** is defined as large quantities (aggregated or associated) of OFFICIAL information related to a Contract/Project that, if lost or compromised, may cause significant impact to Defence. *In the case of AWE's Official Information this will include specified Personal and/or Sensitive Personal Data; or aggregated Data.*

reasonable steps to make sure that all individuals employed on any work in connection with the contract have notice that these statutory provisions apply to them and shall continue to apply after the completion or earlier termination of the contract.

Disclosure of Official Information

15. Disclosure of AWE's information shall be strictly in accordance with the "Need to Know" principle. This principle states that AWE information should only be held by those individuals who are so authorised and have a need for access to it for the efficient discharge of their duties, and in those areas where there are appropriate arrangements to protect it.

16. In order to prevent unauthorised disclosure, AWE's information should not be read or worked on in public places such as on public transport or in cafés or motorway service areas.

17. Except with the written consent of AWE, the contractor shall not disclose the contract (or any provision thereof) to any person other than a person employed by the contractor or in accordance with Paragraph 32 below. It shall be confined to those members of staff whose access to the information is essential for the purpose of their duties.

Storage of AWE Information

18. When not in use, AWE information shall be stored in such a manner to prevent unauthorised disclosure. Information should not be left where it could be viewed by unauthorised persons (eg plans fixed to walls, etc). In the case of Reportable OFFICIAL and/or OFFICIAL-SENSITIVE documents, they must be stored under lock and key in a suitable drawer, cupboard or cabinet.

Security Marking of AWE information

19. As part of the transition to GSC, AWE is taking a position that information classified as OFFICIAL should be marked. This may not always be appropriate, and this position will be subject to review.

20. Information classified as OFFICIAL-SENSITIVE should always bear a security marking.

Use of Communications and IT Systems (CIS)

21. If the contractor is required to receive, store, process or forward Official Information on any PC, Laptop or other IT system, that system must be designed, implemented and operated securely. The risk to the loss or compromise of AWE's information should be understood and an appropriate robust risk management system should be in place. Further guidance is shown in Annex A.

Use of Removable Media

22. Removable media should only be used for data transfer and not for storage. All transfer of data using removable media (eg CD, DVD, etc) should be kept to an absolute minimum and only undertaken when there is a clearly defined business imperative. All media used for Reportable OFFICIAL or OFFICIAL-SENSITIVE data and information, or media containing

Personal or Personnel data, must be encrypted and given a unique reference number. Advice on approved encryption products is available from the AWE Security Authority.

23. All media must be registered and as a minimum, the following information needs to be recorded and retained for accountability purposes:

    a. What data is held on the media.

    b. A record of the media reference number used.

    c. Its classification.

    d. The password used for encryption.

    e. When, how and to whom the media has been sent.

    f. Confirmation of receipt by addressee.

24. BUFF colour-coded media should be used for AWE information.

Transmission of AWE Information

25. AWE information shall be transmitted, both within and outside company premises, in such a way as to make sure that no unauthorised person has access. If transported by hand, material should be carried in a locked container, such as commercial type briefcase or officially approved box, bag, case or pouch, with an “if found” identification luggage label attached. If sent by post, it may be enclosed by a single envelope and sent by Royal Mail, contractors own, or commercial couriers. The classification of the information should not be identified as such on the envelope (eg do not stamp Reportable OFFICIAL or OFFICIAL SENSITIVE – or any legacy GPMS markings such as PROTECT or RESTRICTED - on the envelope). The envelope should bear a company stamp clearly indicating the originating postal address.

26. Transmission of electronic information via public networks such as the Internet or any other form of electronic connectivity is only permitted for legacy information which was Unclassified under GPMS arrangements; for AWE information which been assessed to be non-sensitive, see Annex B for further guidance on sending information offsite.

27. Advice on the transmission of AWE information abroad or any general advice regarding transmission should be sought from the AWE Security Authority.

Use of Contractor IT Systems Onsite

28. In some cases, the most practicable way of meeting contractual requirement will be to introduce contractor IT systems onto an AWE site. This could include either implementing a Local Area Network, a standalone computer, or bring laptop or other portable equipment onto site, Annex C provides further guidance.

Personnel Security

29. All individuals with access to AWE Reportable OFFICIAL or OFFICIAL-SENSITIVE information at the contractors premises are, as a minimum, required to meet the Baseline Personnel Security Standard (BPSS)[2] and nationality requirements may apply.

30. Those who require regular access to AWE Main Sites or material classified CONFIDENTIAL or above, will require to be security cleared to higher levels, depending on the areas or information to which access is required. Information regarding requirements for higher levels of clearance is available from the AWE Security Authority.

Interpretation

31. Advice regarding the interpretation of the above requirements should be sought from the AWE Security Authority.

Audit

32. Where considered necessary by the AWE Security Authority, the contractor shall permit the AWE Security Authority (or his representatives) to inspect the contractors facilities, processes and other security arrangements, or those of sub-contractors and/or service providers, in order to ensure compliance with these requirements. Where appropriate, the contractor should facilitate any access by the AWE to any sub-contractor or service provider. The AWE Security Authority may make representations to the contractor (or where appropriate any sub-contractor or service provider) if any remedial action is considered appropriate.

Annexes

A. MoD Security Conditions
B. Sending Official Information Offsite
C. Using Contractor IT Systems Onsite
D. Contractor IT Assurance Statement

[2] BPSS has replaced the Basic Check (BC) level of clearance. Guidance on this standard is available at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

Annex A: MoD Security Conditions

This Annex sets out in full the Reportable OFFICIAL and OFFICIAL- SENSITIVE Security Conditions for UK Contracts (as taken from JSP440 v 5 Part 4 Section 4 Chapter 2 Annex N)

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

Definitions

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

Security Grading

2. The Authority shall issue a Security Aspects Letter which shall define the OFFICIAL- SENSITIVE and Reportable OFFICIAL 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.

AWE Supplementary Note

As part of the transition to GSC, AWE is taking a position that information classified as OFFICIAL should be marked. This may not always be appropriate, and this position will be subject to review.

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 Reportable OFFICIAL and OFFICIAL- SENSITIVE Information

4. The Contractor shall protect Reportable 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. Reportable 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 or compromise of the information or from deliberate or opportunist attack.

6. All OFFICIAL-SENSITIVE material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use OFFICIAL-SENSITIVE documents/material shall be stored under lock and key. As a minimum, when not in use, OFFICIAL-SENSITIVE material shall be stored 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.

7. Disclosure of 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.

8. 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 31.

Access

9. Access to Reportable 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.

10. 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

AWE Supplementary Note

AWE expects that any individual having access to AWE Reportable OFFICIAL information should also meet BPSS requirements.

Hard Copy Distribution of Information

11. Reportable 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 Reportable 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.

12. 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.

AWE Supplementary Note

Authority for the offshoring of AWE OFFICIAL, Reportable OFFICIAL or OFFICIAL-SENSITIVE information must be sought from the AWE Security Authority.

Electronic Communication, Telephony and Facsimile Services

13. Reportable OFFICIAL information may be emailed unencrypted to recipients over the internet when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions. OFFICIAL-SENSITIVE information shall normally be transmitted over the internet encrypted using a Foundation Grade or equivalent product. Information about Foundation Grade products and the CESG Commercial Product Assurance scheme is available at:

http://www.cesg.gov.uk/servicecatalogue/Product-Assurance/CPA/Pages/Certified-products.aspx

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.

AWE Supplementary Note

As part of the transition to GSC, AWE is taking a position that information classified as OFFICIAL-SENSITIVE should NOT be transmitted over the Internet without the express permission of the AWE Security Authority.

This position will be subject to review.

14. 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.

15. OFFICIAL-SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not with (or within) earshot of unauthorised persons.

16. OFFICIAL-SENSITIVE information may be faxed to UK recipients.

17. Reportable OFFICIAL information may be discussed with and faxed to recipients located overseas.

AWE Supplementary Note

Authority for the offshoring of AWE OFFICIAL, Reportable OFFICIAL or OFFICIAL-SENSITIVE information must be sought from the AWE Security Authority.

Use of Information Systems

18. The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot 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.

AWE Supplementary Note

AWE expects that any system processing AWE OFFICIAL, Reportable OFFICIAL or OFFICIAL-SENSITIVE information should be subject to an appropriate information risk management regime.

HMG Guidance is available at:

https://www.gov.uk/government/publications/technology-and-information-risk-management

AWE expects that the contractor will provide a written assurance statement to the effect that any system – either belonging to the contractor, to any sub-contractor - processing AWE Reportable OFFICIAL or OFFICIAL-SENSITIVE information is subject to an appropriate information risk management regime. There is no requirement to provide this written assurance for OFFICIAL only working.

19. 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.

20. 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 Foundation Grade 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
(h) 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.

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

1. Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and 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,

h. 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"

i. 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.

j. 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) which is acceptable to the Authority's Principal Security Advisor.

k. 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

21. Laptops holding any MOD supplied or contractor generated Reportable OFFICIAL and OFFICIAL-SENSITIVE information are to be encrypted using a Foundation Grade product or equivalent as described in paragraph 13 above.

AWE Supplementary Note

All laptops holding any AWE OFFICIAL, Reportable OFFICIAL or OFFICIAL-SENSITIVE information must be protected by full disk encryption. The minimum standard to be used is a FIPS 140-2 encryption product.

22. Unencrypted laptops not on a secure site1 are to be recalled and only used or stored in an appropriately secure location until further notice or until 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.

23. 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.

24. 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

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

AWE Supplementary Note

Any security incident involving only AWE OFFICIAL should be reported as soon as practical to the

relevant AWE Contract Manager/Project Manager.

Any security incident involving any Reportable OFFICIAL or OFFICIAL-SENSITIVE information should be reported immediately to the AWE Security Authority and then to the relevant AWE Contract Manager/Project Manager.

AWE will provide subsequent guidance on any additional reporting or incident procedures that the contractor may be required to take.

26. Any security incident involving any MOD owned, processed, or contractor generated Reportable 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.uk
Telephone: Working Hours: 030 677 021 187
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

27. 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 Reportable OFFICIAL or OFFICIAL-SENSITIVE 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 form can be found at Appendix 5 at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/299557/Contractual_Process.pdf

If the Sub-contract is approved, the Authority shall provide the Contractor with the security conditions that shall be incorporated within the Sub-contract document.

Publicity Material

28. 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

29. 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 to DBR-DefSy(S&T/Ind) for PV Security Grading in accordance with the requirement detailed at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/300050/pv_grading_flyer_apr14.pdf

Promotions and Potential Export Sales

30. 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

31. As soon as no longer required, Reportable 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

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

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

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

Audit

34. 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.

Annex B: Sending AWE information Offsite

General

B1. AWE information should only be sent offsite in support of a genuine business requirement. All the following conditions should be met:

a. The appropriate **contractual cover** has been established.

b. The receiving contractor/organisation is **correctly authorised** and **competent** to hold that information.

c. The information is **correctly classified (**as defined by a classifications officer or AWE project specific guidance document)

d. The information is of a classification that allows it to be **removed from site.**

e. The information is sent offsite in an **approved manner.**

B2. This Annex describes the approved export mechanisms and supporting procedural controls that should be in place.

Business Requirement

B3. In some instances, contractual arrangements will specify that AWE information may be held and/or processed by third party contractors. That should be clearly defined in any Security Aspects Letter (SAL) that is issued to the contractor. The AWE Project Sponsor is required to ensure that only the minimum amount of AWE's information required to discharge the contractual requirement is released to the contractor.

Contractual Cover

B4. An appropriate contractual arrangement, supported by a Security Aspects Letter, (SAL), must be in place. [*NB that any contractual arrangements which involve offsite working with AWE information above OFFICIAL must be done under List X arrangements*.]

Receiving Organisation

B5. The AWE Project Sponsor should be satisfied that the receiving organisation is made aware of, and understands, the measures that should be in place to protect the AWE information. That assurance may be provided by the receiving organisation, or may be provided by an acceptable Agency which has already undertaken an independent assessment of arrangements in place at the contractor premises. If there is any doubt about the receiving contractors/organisation's competence in this area, AWE can, and should, provide appropriate guidance and an assessment of an organisation's suitability to protect AWE's information.

Protective Marking

B6. The AWE Project Sponsor should ensure that a Local Classifications Officer (LCO) is nominated and a Project Classification Guide (PCG) is provided. That guide should incorporate existing HMG/MoD/AWE policies and guidelines on the classification of information, and should provide clear guidance for contractors/project staff to allow them to correctly classify information.

Personal Data

B7. Where Personal Data is involved, additional security measures will apply. AWE is required to protect personal information from unauthorised access, release or loss, which includes any Personal Data cascaded to, or by, contractors. Individuals who have authorised access to, or management responsibility for, Personal Data need to undergo appropriate training annually with their respective companies/organisations. In addition, any system which processes personal information must be subject to a Privacy Impact Assessment (PIA) carried out by or on behalf of the AWE Security Authority. PIAs need to be reviewed annually or when there is any material change to the system.

Offshoring AWE Information

B8. Where there is a requirement to store, process, or access AWE's information outside the UK, or to have access to any contractor system which includes AWE information, a risk assessment should be carried out by, or on behalf of, the AWE Security Authority.

Approved Systems

B9. Where OFFICIAL-SENSITIVE material is required to be sent offsite, only approved systems (export mechanisms) may be used to transmit that material, and only when the AWE Project Sponsor is satisfied that the receiving organisation is able to hold and/or process that information.

Export Mechanisms

B10. The order of preference is that AWE information should be exported by secure and direct electronic means; by secure indirect electronic means; or by media transfer. Where a contractor has SECURE email connectivity (eg via the RLI or GSi), the preferred route for OFFICIAL-SENSITIVE information will be via email transfer (either direct from an approved onsite system or indirectly via an approved transfer mechanism).

B11. OFFICIAL material may be sent via the Internet.

Contractor Monitoring

B12. Where considered appropriate, contractor staff working onsite may be subject to additional monitoring controls, and/or limited onsite system privileges. This could include not having internet access from AWE systems; not having media export/creation rights; and externally-released emails being routed through and/or copied to the AWE Project Sponsor or his/her representative.

Annex C: Using Contractor IT Systems Onsite

Definition

C1. A contractor system is any non-AWE system (including local area networks, standalone computers, laptops, handheld devices, etc) used to store, process, access or forward information; or used to support or maintain any contractor - or AWE-owned system or equipment.

General

C2. Contractor systems may only be brought onto site in support of an authorised AWE business requirement, or for contractor internal administration purposes, providing that relevant AWE authority has been granted and that the system has been registered with AWE.

Authority to Operate

C3. All systems MUST be registered with the AWE IT Security Officer.

C4. All systems in use must either be formally accredited (see below) and/or given Authority to Operate (ATO) by AWE, or be under an arrangement recognised and/or approved by AWE.

C5. Under no circumstances may privately-owned systems, or systems not under the effective control of a contractor, be used in support of any contractor-supplied services; be used to process AWE information; or be used to support or maintain any other equipment onsite.

C6. All systems must be operated in accordance with their Security Operating Procedures (SyOPs) (or equivalent document).

C7. Use of contractor systems must be in accordance with AWE installation and design requirements, and with AWE's Zoning Policy.

Accreditation Requirement

C8. The following table lists the responsibility for providing formal Accreditation or Approval to Operate (ATO).

Classification	Registration	Accreditation Requirement
UNCLASSIFIED	**YES** All systems used onsite MUST be registered with AWE	*Formal accreditation not required. This legacy GPMS marking will not be used by AWE after 1st April 2015.*
OFFICIAL		**Formal accreditation NOT required. Contractors should provide an assurance statement to AWE: see AWE Supplementary Note to Annex A paragraph 18**
PROTECT *RESTRICTED*		*These legacy GPMS markings will be not used by AWE after 1st April 2015.*
CONFIDENTIAL		*This legacy GPMS classification will continue to be used by AWE beyond 1st April 2015. Additional guidance is available for contractors working at this level.*
SECRET **TOP SECRET**		**DAIS (MoD Accreditation Authority)**

Annex D: Contractor IT Assurance Statement

You are only required to submit this Assurance Statement if your company is working at the OFFICIAL-SENSITIVE classification. It is NOT required for OFFICIAL only work.

Return Address:

AWE List X Advisor
F6.1
AWE
Aldermaston
Reading
Berks RG7 4PR

Company name	
Company representative providing assurance	
Brief details of system (name etc)	

On behalf of (*name of company*) I [*name*] conform that the system identified above meets the requirements specified in the AWE Supplementary Note to Annex A Paragraph 18, and shall be the only system(s) used to process AWE **Reportable OFFICIAL** or **OFFICIAL-SENSITIVE** information.

This form should be adapted as required to provide an assurance statement on behalf of sub-contractors/in respect of sub-contractor systems processing AWE **OFFICIAL-SENSITIVE** information.