Joint Maritime Security Centre

Joint Maritime Security Centre
A Leg, Navy Command HQ (Portsdown Hill)
QinetiQ Portsdown Technology Park
Southwick Hill Road
Cosham
Hampshire
P06 3RU

michael.allen@homeoffice.gov.uk

[redacted]

Joint Maritime Security Centre - GOV.UK (www.gov.uk)

Carbon60 Ltd
3600 The Solent Centre
Fareham
PO15 7AN

16th June 2025

SUBJECT: SECURITY ASPECTS LETTER (SAL)

1. This letter sets out certain security provisions which Carbon60 (The **Supplier**) must comply with when delivering services and support to The Home Office, (The Authority) in relation to the contract **Digital Maritime Security Capabilities** in support of the Joint Maritime Security Centre.

2. This letter sets out certain security provisions which the Supplier must comply with when providing support to the Authority. It explains the Supplier responsibilities when dealing with His Majesty's Government (HMG) information assessed as OFFICIAL, OFFICIAL - SENSITIVE, or SECRET in accordance with the Government Security Classifications policy, May 2018. Government Security Classifications - GOV.UK (www.gov.uk)

3. The aspects, as set out below, must be fully safeguarded. The enclosed Security Condition (see attached copy of Annex A) outlines the minimum measures required to safeguard OFFICIAL – SENSITIVE assets and information.

4. The bulk of the information processed by the Supplier relating to **Digital Maritime Security Capabilities** is expected to be classified up to OFFICIAL - SENSITIVE. The Supplier will therefore implement controls appropriate to maintain the security of all live data streamed and relative components whether these be physical document store or electronic information storage
   A Certificate of Deletion of any stored data will be issued upon completion.

5. Data which is entrusted to The Supplier and its partners and sub-contractors must be protected by The Supplier and its partners and sub-contractors in accordance with the requirements contained within HMG Security Policy Framework and comply with the relevant standards and guidance published by National Cyber Security Centre (NCSC) and National Protective Security Authority (NPSA).

6. Where The Supplier undertake sub-contracting or “routes to market” activities in accordance with the terms of the Contract, The Supplier shall ensure that a SAL on equivalent terms to this SAL shall be entered into by The Supplier and the relevant subcontractor.

7. For the avoidance of doubt any reference in this SAL to “Employee” means any of The Supplier employees, partners, 3rd party support staff, agents, officers, directors, or secretaries supporting the delivery of services to the JMSC Tracks Service or to organisations associated with The Authority and JMSC.

8. This SAL supersedes any previous SAL that The Supplier may have received in relation to this programme of work.

9. The Supplier should consult with JMSC Project Management Office (PMO) immediately where any doubt exists as to the protection necessary to safeguard any classified material.

10. The Supplier must report immediately to the Home Office Senior Information Risk Owner, via the JMSC Information Assurance Team (contact details below) any incident or information that raises doubts as to compliance with the terms of this SAL.

    Joint Maritime Security Centre Information Assurance team:

    [redacted]
    JMSC
    Portsdown Technology Park,
    Cosham,
    PO6 3RU
    Email: [redacted] or jmscinformationmanagementteam@jmsc.gov.uk
    Tel: [redacted]

Government Security Classifications

11. All information provided by The Authority for the purposes of the Digital Maritime Security Capabilities unless otherwise marked shall be treated as OFFICIAL.

12. All Government information has a value so the terms NOT CLASSIFIED or NPM must NOT be used. Government furnished information (whether marked or unmarked) must be treated as a minimum of OFFICIAL.

13. The SENSITIVE caveat is used to denote OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the ‘need to know’. The Security Aspects Letter, issued by the Authority shall define the OFFICIAL-SENSITIVE material that is provided to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all OFFICIAL and OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable Government Security Classification (GSC).

14. Consequently, access to OFFICIAL - SENSITIVE information must be no wider than necessary for the efficient conduct of The Supplier obligations under the Contract and limited to those with a business need and the appropriate security clearances. This “need to know” principle applies wherever SENSITIVE information is collected, stored, processed, or shared.

15. OFFICIAL - SENSITIVE information may sometimes include a descriptor to identify categories

of sensitive information and indicate the need for common sense precautions to limit access, The descriptor COMMERCIAL indicates the information contains commercial or market-sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed.

16. As identified in Paragraph five, The Supplier may occasionally handle documents which will attract a classification higher than OFFICIAL, for example, where certain specific stakeholders are identified, or current or future capability gaps are described. If The Supplier is required to handle or process information that is more highly classified, they must contact the JMSC Information Assurance Team to determine how to manage the information.

17. All non-UK nationals proposed by The Supplier to work on the provision or delivery of services to the JMSC Programme must provide their security clearance details to the JMSC HO Security Officer, via the PMO for verification.

18. Any data or documents that are issued to The Supplier with a caveat of 'UK Eyes Only' must not be accessed or viewed by any member of staff who has a restriction on their clearance preventing access to UKEO material.

GUIDANCE ON CLASSIFICATION OF INFORMATION TYPES

19. The following table defines the commensurate classification requirements to apply to a non-exhaustive list of aspects relating to the Digital Maritime Security Capabilities. It is expected that the classification of material or capabilities developed through and by The Supplier can be extrapolated by The Supplier from this list. In the list below the classifications apply to the aspects taken in isolation, if we hold all the information in one place the classification will not raise above OFFICIAL.

ASPECT (Non Exhaustive)	CLASSIFICATION	HANDLING CAVEAT
Government data	OFFICIAL	SENSITIVE
Third Party data	OFFICIAL	COMMERCIAL
[redacted]	[redacted]	[redacted]

Commented [KF1]: Completed

Table 1: Detailed schedule of classification

Notes

- Where the classifications above differ for a particular aspect, this is indicative that the precise sensitivity and detail of the aspect should be considered. It is the responsibility of both The Supplier and JMSC Leads to ensure that the appropriate classification is correctly applied.
- Where a document is supplied to The Supplier by the Authority with an existing protective marking or classification that classification or marking may not be changed and no extract from that document may be added to a document at a different classification without the permission of the author of the document.

20. Your attention is drawn to the provisions of the Official Secrets Act 1911-1989 in general, and specifically to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989). In particular you should take all reasonable steps to make sure that all

individuals employed on any work in connection with this Contract have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply after completion or earlier termination of the contract

21. Will you please confirm that:

    a. This definition of the classified aspects of the referenced Contract has been brought to the attention of the person directly responsible for security of classified material.

    b. The definition is fully understood.

    c. Measures can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations. [The requirement and obligations set out above and in any contractual document can and will be met and that the classified information shall be protected in accordance with applicable national laws and regulations.]

    d. All employees of the company who will have access to classified information have either signed the Official Secrets Act (OSA) Declaration Form in duplicate and one copy is retained by the Company Security Officer or have otherwise been informed that the provisions of the OSA apply to all classified information and assets associated with this contract.

22. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, you will discuss with the authority immediately .

23. Classified Information associated with this Contract must not be published or communicated to anyone without the written approval of the Authority.

24. Any access to classified information or assets on The Authority premises that may be needed will be subject to The Authorities security regulations under the direction of the JMSC Project Officer in accordance with the HMG Security Policy Framework.

Yours faithfully

[redacted]
Joint Maritime Security Centre

ANNEX A:

OFFICIAL AND OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS

Purpose

1. This document provides guidance for Contractors where classified material provided to or generated by the Contractor is graded OFFICIAL or OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the JMSC Data Compliance & Security Officer.

Definitions

2. The term "Authority" for the purposes of this Annex means the HMG Contracting Authority.

3. The term "Classified Material" for the purposes of this Annex means classified information and assets.

Security Classification

4. The SENSITIVE caveat is used to denote OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the ‘need to know’. Where OFFICIAL-SENSITIVE material requires additional protection or additional preventative security controls the Authority will stipulate these requirements if and when they are required. The Security Aspects Letter, issued by the Authority shall define the OFFICIAL-SENSITIVE material that is provided to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all OFFICIAL and OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security classification

Security Conditions

5. The Contractor shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex. The Contractor shall make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and shall continue so to apply after the completion or earlier termination of the Contract. The Authority must state the data retention periods to allow the Contractor to produce a data management policy. If you are a Contractor located in the UK your attention is also drawn to the provisions of the Official Secrets Acts 1911 to 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.

Joint Maritime Security Centre

Annex B – Home Office Classification and Handling Instructions

	OFFICIAL *Minimum* controls include:	SECRET *Additional* minimum controls include:	TOP SECRET *Additional* minimum controls include:
Personnel Security	• Appropriate recruitment checks (e.g., CTC or BPSS) • Reinforce personal responsibility and duty of care through induction training. • "Need to know" for sensitive assets	• [redacted] if and when required	• Details provided if and when required
Storage	• Clear desk / screen policy • Consider proportionate measures to control and monitor access to more sensitive assets Storage under single barrier and / or lock and key • Consider use of appropriate physical security furniture such as CPNI class 1	• Details provided if and when required •	• Details provided if and when required
Remote Working	• Ensure information cannot be inadvertently overlooked whilst being accessed remotely • Store more sensitive assets under lock and key at remote locations	• Details provided if and when required.	• Details provided if and when required

	OFFICIAL *Minimum* controls include:	SECRET *Additional* minimum controls include:	TOP SECRET *Additional* minimum controls include:
Moving assets by hand or by post (within UK)	• Single cover • Precautions against overlooking when working in transit • Authorisation required from line managers for significant volume of records/files that may affect aggregate classification or associated risk of loss or compromise. For post: • Include return address, never mark classification on envelope • Consider double envelope for sensitive assets • Consider using registered Royal Mail service or reputable commercial courier's "track and trace" service	• Details provided if and when required	• Details provided if and when required
Moving assets overseas (by hand or post)	• Only subject to operational requirement • By trusted hand under single cover • Include return address, never mark classification on envelope • Consider double envelope for sensitive assets • Consider using registered Royal Mail service or reputable commercial courier's "track and trace" service	• Details provided if and when required	• Details provided if and when required

	OFFICIAL *Minimum* controls include:	SECRET *Additional* minimum controls include:	TOP SECRET *Additional* minimum controls include:
Bulk Transfers	• Local management approval (Chief Inspector and equivalent), • Consider appropriate risk assessment and movement plans. • Consider aggregation of data / assets and handle in line with aggregated handling. • Home Office CSAS Bulk Data for OFFICIAL definition: One full removal crate.	• Details provided if and when required	• Details provided if and when required
Electronic Information at Rest	• Electronic Information will be protected at rest by appropriate physical protection (such as Home Office accredited accommodation) Foundation Grade data at rest encryption when physical control is not guaranteed (such as bit locker on a laptop)	Details provided if and when required	Details provided if and when required.

	OFFICIAL *Minimum* controls include:	SECRET *Additional* minimum controls include:	TOP SECRET *Additional* minimum controls include:
Electronic Information in Transit	• Information in transit between Government or other trusted orgainsation's will be via accredited shared infrastructure (such as PSN) or protected using Foundation Grade encryption • OFFICIAL may be emailed / shared unprotected to external NGO partners / citizens, subject to local business policies and procedures • Where more sensitive information must be shared with external partners, consider using secure mechanisms (e.g., browser sessions using SSL / TLS) in line with industry security practices.	• Details provided if and when required	• Details provided if and when required
ICT Services (Each CT Network System / Service will have its own Accreditation and Security Procedures which clarify specific requirements.)	• Different GCloud services will be suitable for different types of OFFICIAL information. Risk owners MUST read and understand any GCloud accreditation residual risk statements • End user devices will conform to the security principles defined in the Home Office Acceptable Use Policy	Details provided if and when required	• Details provided if and when required

	OFFICIAL *Minimum* controls include:	SECRET • *Additional* minimum controls include:	TOP SECRET *Additional* minimum controls include:
Removable Media	• The use of removable media will be minimized. Other approved information exchange mechanisms should be used where available in preference • NCSC approved Foundation Grade encryption is recommended or FIPS 140-2 equivalent may be appropriate (where it is outside the organization's physical control)	• Details provided if and when required	• Details provided if and when required.
Telephony (mobile and landline), Video Conference and Fax	• Use of accredited solutions such as secure Chorus products. • Freeware and untrusted platforms should **not** be used (including WhatsApp) • Details of sensitive material should be kept to a minimum • Recipients should be waiting to receive faxes	• Details provided if and when required	Details provided if and when required
Disposal / Destruction	• Dispose of with care using a shredder to make reconstitution difficult.	Details provided if and when required	• Details provided if and when required