[redacted]

Our Ref: [redacted]

Date: 28/07/2022

For the personal attention of: [redacted]

Security Aspects Letter (SAL) for Invitations to Tender (ITT) for Contracts Involving Information Classified OFFICIAL and OFFICIAL-SENSITIVE but not above to UK Firms

Dear Sirs,

TENDER NUMBER AND SUBJECT: ND2 Neurodiversity Support and Awareness

DATE OF ITT: 27/05/2022

DESCRIPTION: We wish to establish a new **Neurodiversity Support and Awareness Framework Agreement.** This will enable us to call upon specialist provider(s) for a wide range of neurodiversity services and training. For example: non-clinical assessments; one-to-one coaching for neurodiverse individuals and/or line managers; specialist advice for workplace adjustments; equality impact assessments; support to organisational change programmes; and design and delivery of awareness training for staff and line managers.

1. On behalf of the Secretary of State for Defence I hereby give you notice of the information or assets connected with, or arising from, the referenced ITT that constitute classified material.
2. Aspects that constitute OFFICIAL-SENSITIVE for the purposes of DEFCON 660 are specific below. These aspects must be fully safeguarded.

[redacted]

3. 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 ITT have

notice of the above specific aspects and that the aforementioned statutory provisions apply to them and will continue to apply should the ITT be unsuccessful.

4. Will you please confirm, in writing, that:

   - This definition of the classified aspects of the referenced invitation to Tender has been brought to the attention of the person directly responsible for security of classified material.
   - The definition is fully understood.
   - The requirements and obligations set out herein 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.
   - All employees of the company who will have access to classified information heave either signed the OSA Declaration Form or a statement acknowledging the OSA, during the invitation to tender, the term of the contract if awarded and after its completion or termination. This is required in duplicate with one copy retained by the Company Security Controller.

   Confirmation, quoting the tender number and subject, is to be sent to:

   Please confirm this through the DSP E Tendering Portal

5. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.

6. Classified information associated with this ITT must not be published or communicated to anyone without the approval of the MOD Contracting Authority.

7. Any access to information on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer.

8. DEFCON 660 – OFFICIAL-SENSITIVE Security Requirements and the principal measures required to safeguard OFFICIAL and OFFICIAL-SENSITIVE information are appended at Annexes A and B for your information.

9. DEFCON 531 – Disclosure of Information applies to this contract and a copy is appended at Annex C for ease of reference.

10. Where there is a requirement to forward information relating to the contract to Dstl using removable IT media (e.g. CD, DVD, USB drive) such media must be encrypted. At classifications of OFFICIAL and OFFICIAL-SENSITIVE, the media is to be encrypted using: See Annex D for additional details on appropriate encryption products.

11. All Government Furnished Information (GFI) documents provided by MOD in support of this contract (including all copies and extracts therefrom) are, on completion or earlier termination of the contract, to be returned to Dstl

Yours sincerely

[redacted]

[redacted]

Copy via email to:

- The Demander
- [redacted]

[redacted]

[redacted]

Annex A

DEFCON 660 – OFFICIAL-SENSITIVE SECURITY REQUIREMENTS

1. In this condition 'Information' means information recorded in any form disclosed or created in connection with the contract.
2. The Contractor shall protect all Information relating to the aspects designated OFFICIAL-SENSITIVE as identified in the security aspects letter annexed to the Contract, in accordance with the official security conditions contained in the contract or annexed to the Security Aspects Letter.
3. The Contractor shall include the requirements and obligations set out in clause 2 in any sub-contract placed in connection with or for the purposes of the Contract which requires disclosure of OFFICIAL-SENSITIVE information to the sub-contractor or under which any information relating to aspects designated as OFFICIAL-SENSITIVE is created by the sub-contractor. The Contractor shall also include in the sub-contract a requirement for the sub-contractor to flow the requirements of this clause to its sub-contractors and through all levels of the supply chain to the lowest level where any OFFICIAL-SENSITIVE information is handled.

Use of the OFFICIAL-SENSITIVE LIMCIRC (limited circulation) Handling Instruction

1. The Handling Instruction 'Limited Circulation' (abbreviated to LIMCIRC) is used to provide a system for ensuring that specific OFFICIAL-SENSITIVE information is exposed only to those with a strict 'need to know'.
2. A LIMCIRC documents must be clearly marked as such (OFFICIAL-SENSITIVE LIMCIRC in the document headers and footers) and must contain the expression 'Handling Instruction: Limited Circulation' beneath the classification in the headers. A defined distribution list, i.e. by name or appointment is to be included with every document carrying the LIMCIRC handling instruction.
3. It is accepted that outer office staff, e.g. secretarial staff, personal assistants, etc. of named recipients will be authorised to see/handle such documents without being specifically named on the distribution list.
4. Recipients of LIMCIRC documents must not circulate the document further without the explicit approval from the originator or someone authorised to act on their behalf. Protections appropriate for OFFICIAL-SENSITIVE information must be fully enforced.
5. OFFICIAL-SENSITIVE and OFFICIAL-SENSITIVE LIMCIRC material may not be transmitted over the internet without the use of MOD approved encryption. Anyone transmitting LIMCIRC material should ensure that any covering email contains the expression 'Handling Instruction: Limited Circulation'.
6. Conversations involving OFFICIAL-SENSITIVE LIMCIRC material must only be conducted in an environment where they cannot be overheard by those without a 'need to know'.
7. Failure to safeguard OFFICIAL-SENSITIVE LIMCIRC information or assets, or unauthorised distribution or disclosure of LIMCIRC information both fall under the security breach category 'serious breach'.

Annex B

OFFICIAL and OFFICIAL-SENSITIVE SECURITY CONDITIONS

Purpose

1. This document provides guidance for Contractors where classified material provided to or generated by the Contractor is graded UK OFFICIAL or UK OFFICIAL_SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (email: [redacted]

Definitions

2. The term 'Authority' for the purpose 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 Grading

4. The SENSITIVE caveat is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the 'need to know'. This Security Aspects Letter, issued by the Authority defines the UK 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 UK OFFICIAL and UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading.

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 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 and 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.

Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE information

6. The Contractor shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material 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 classified material whether accidentally or from deliberate or opportunistic attack.
7. Once the Contract has been awarded, where Contractors are required to store or process UK MOD classified information electronically, they are required to register the IT system onto the Defence Assurance Risk Tool (DART). Details on the registration process can be found in the 'Industry Security Notices (ISN)' on Gov.UK website. ISNs 2017/01, Defence Condition 658 and Defence Standard 05-138 details the DART registration, IT

security accreditation processes, risk assessment/management and Cyber security requirements which can be found in the following links:

- [redacted]

[redacted]

8. All UK classified material including documents, media, and other assets must be physically secured to prevent unauthorised access. When not in use UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be subject to a level of control.
9. Disclosure of UK OFFICIAL and UK OFFICIAL-SENSITIVE material must be strictly controlled in accordance with the 'need to know' principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Contractor or sub-Contractor.
10. Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any information issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 9 above, the Contractor shall not make use of any article or part thereof similar to the articles for any other purpose.
11. Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Contractor from using any specifications, plans, drawings and other documents generated outside of this Contract.
12. 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 must be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 35.

Access

13. Access to UK OFFICIAL and UK OFFICIAL-SENSITIVE material 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 their duties.
14. The Contractor shall ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE information have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

[redacted]

Hard Copy Distribution

15. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents shall be distributed, both within and outside Contractor premises in such a way as to make sure that no unauthorised

person has access. It may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must **not** appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial couriers may be used.

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

Electronic Communication, Telephony and Facsimile Services

17. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or a UK 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:

[redacted]

Details of the CPA scheme are available at:

[redacted]

18. **Exceptionally**, in urgent cases, UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the **prior** approval of the Authority. However, it 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 require. Such limitations including any regarding publications, further circulation, or other handling instructions shall be clearly identified in the email sent with the material.
19. UK OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the country of the Contractor and overseas. UK OFFICIAL-SENSITIVE information may be discussed on fixed and mobile telephones only where there is a strong business need to do so and only with the prior approval of the Authority.
20. UK OFFICIAL information may be faxed to recipients located both within the country of the Contractor and overseas; however UK OFFICIAL-SENSITIVE information may be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

Use of Information Systems

21. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here in specific detail; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.
22. 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 UK OFFICIAL or UK OFFICIAL-SENSITIVE information. The Contractor should ensure that competent personnel apply 10 Steps to Cyber Security, which is available at:

[redacted]

23. 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.

24. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing UK 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:

        i. Up to date lists of authorised users.

        ii. Positive identification of all users at the start of each processing session.

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

    d. Internal Access Control – All systems are to have Internal Access Controls to prevent unauthorised users from accessing or modifying the data.

    e. Data Transmission – Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only 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 17 above,

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

        i. The following events shall always be recorded:

            1. All log on attempts whether successful or failed
            2. Log off (including time out where applicable)
            3. The creation, deletion or alteration of access rights and privileges
            4. The creation, deletion or alteration of passwords.

        ii. For each of the events listed above, the following information is to be recorded:

            1. Type of event
            2. User ID
            3. Date & time
            4. Device ID

        The accounting records are to have a facility to provide the System Manager with a hard copy of all or selected activity. There also must 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 must 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 are to be implemented:

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

   ii. Defined Business Contingency Plan,

   iii. Data backup with local storage,

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

   v. Operating systems, applications and firmware should be supported,

   vi. Patching of Operating Systems and Applications used are to 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 must 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).

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

Laptops

25. Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 17 above.

26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites[1]. For the avoidance of doubt the term 'drives' includes all removable, recordable media, e.g. memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

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

27. 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.

28. Portable CIS devices holding the Authorities' data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicle 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 opportunistic theft.

Loss and Incident Reporting

29. The Contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIAL-SENSITIVE information to the Authority. In addition any loss or otherwise compromise of any UK MOD owned, processed or UK MOD Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC) below. 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 UK MOD's Chief Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD WARP will also advise the Contractor what further action is required to be undertaken.

JSyCC WARP Contact Details

RLI Email: For those with access to the RLI: [redacted](MULTIUSER)

Email: [redacted](OFFICIAL with no NTK restrictions))

Telephone (Office Hours): [redacted]

[redacted]

[redacted]

30. Reporting instructions for any security incidents involving MOD classified material can be found in [redacted] as may be subsequently updated at:

[redacted]

Sub-Contracts

31. Where the Contractor wishes to sub-contract any elements of a Contract to sub-Contractors within its own country or to Contractors located in the UK such sub-contracts will be notified to the Contracting Authority. The Contractor shall ensure that these Security Conditions are incorporated within the sub-contract document.

32. The **prior** approval of the Authority shall be obtained should the Contractor wish to sub-contract any UK OFFICIAL-SENSITIVE elements of the Contract to a Sub-contractor located in another (third party) country. The first page of Appendix 5 (MOD Form 1686 (F1686)) of the GovS 007 Security Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at Appendix 5 at:

[redacted]

33. If the sub-contract is approved, the Contractor will flow down the Security Conditions in line with paragraph 31 above to the sub-Contractor. Contractors located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

Publicity Material

34. Contractors wishing to release any publicity material or display hardware that arises from a Contract to which these Security Conditions apply must 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 UK Government.

Physical Destruction

35. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, 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 UK OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

36. Advice regarding the interpretation of the above requirements should be sought from the Authority.
37. Further requirements, advice and guidance for the protection of UK classified information at the level of UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

[redacted]

Audit

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

Annex C

DEFCON 531 – DISCLOSURE OF INFORMATION

1. ‘Information’ means any information in any written or other tangible form disclosed to one party by or on behalf of the other party under or in connection with the Contract, including information provided in the tender or negotiations which preceded the award of the Contract.

2. Subject to Clause 5 to 10 each party:

   a) Shall treat in confidence all Information it receives from the other;

   b) Shall not disclose any of that Information to any third party without the prior written consent of the other party, which consent shall not unreasonably be withheld, except that the Contractor may disclose Information in confidence, without prior consent, to such persons and to such extent as may be necessary for the performance of the Contract;

   c) Shall not use any of that Information otherwise than for the purpose of the Contract; and

   d) Shall not copy any of that Information except to the extent necessary for the purpose of exercising its rights of use and disclosure under the Contract.

3. The Contractor shall take all reasonable precautions necessary to ensure that all Information disclosed to the Contractor by or on behalf of the Authority under or in connection with the Contract:

   a) Is disclosed to their employees and sub-contractors, only to the extent necessary for the performance of the Contract; and

   b) Is treated in confidence by them and not disclosed except with prior written consent or used otherwise that for the purpose of performing work or having work performed for the Authority under the Contract or any sub-contract under it.

4. The Contractor shall ensure that their employees are aware of their arrangements for discharging the obligations at Clauses 2 and 3 before they receive Information and take such steps as may be reasonably practical to enforce such arrangements.

5. A party shall not be in breach of Clauses 2, 3, 7, 8 and 9 to the extent that either party;

   a) Exercises rights of use or disclosure granted otherwise than in consequence of, or under, the Contract;

   b) Has the right to use or disclose the Information in accordance with other conditions of the Contract; or

   c) Can show:

      i. that the Information was or has become published or publicly available for use otherwise than in breach of any provision of the Contract or any other agreement between the parties;

      ii. that the Information was already known to it (without restrictions on disclosure or use) prior to it receiving it under or in connection with the Contract;

iii. that the Information was received without restriction on further disclosure from a third party who lawfully acquired it and who is himself under no obligation restricting its disclosure; or

iv. from its records that the same information was derived independently of that received under or in connection with the Contract;

provided the relationship to any other Information is not revealed.

6. Neither party shall be in breach of this Condition where it can show that any disclosure of Information was made solely and to the extent necessary to comply with a statutory, judicial or parliamentary obligation. Where such a disclosure is made, the party making the disclosure shall ensure that the recipient of the Information is made aware of and asked to respect its confidentiality. Such disclosure shall in no way diminish the obligations of the parties under this Condition.

7. The Authority may disclose the Information:

a) to any central government body for any proper purpose of the Authority or of the relevant central government body, which shall include: disclosure to the Cabinet Office and/or HM Treasury for the purpose of ensuring effective cross-Government procurement processes, including value for money and related purposes. Where such a disclosure is made the authority shall ensure that the recipient is made aware of its confidentiality

b) to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;

c) subject to Clause 8 below, to the extent that the Authority (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;

d) subject to Clause 8 below, on a confidential basis to a professional adviser, consultant or other person engaged by any of the entities defined in DEFCON 501 (including benchmarking organisation) for any purpose relating to or connected with this Contract;

e) on a confidential basis for the purpose of the exercise of its rights under the Contract; or

f) on a confidential basis to a proposed body in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under the Contract;

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent that those placed on the Authority under this DEFCON.

8. Where the Authority intends to disclose Information to a commercial entity which is not a Central Government Body in accordance with Clauses 7.c or 7.d above, the Authority will endeavour to provide the Contractor with 3 Business Days' notice in advance of such disclosure. In relation to a disclosure of Information made under Clause 7.c above, if reasonably requested by the Contractor within 2 Business Days of such notice being given, where the Authority has not already done so, it will endeavour to procure from the intended recipient of the Information an agreement containing confidentiality terms the same as, or substantially similar to, those placed on the Authority under this DEFCON.

9. Before sharing any Information in accordance with clause 7 above, the Authority may redact the Information. Any decision to redact information made by the Authority shall be final.

10. The Authority shall not be in breach of the Contract where it can show that any disclosure of Information is made solely and to the extent necessary to comply with the Freedom of Information Act 2000 ("the Act") or the Environmental Information Regulations 2004 ("the Regulations"). To the extent permitted by the time for compliance under the Act or the Regulations, the Authority shall consult the Contractor where the Authority is considering the disclosure of Information under the Act or the Regulations and, in any event, shall provide prior notification to the Contractor of any decision to disclose the Information. The Contractor acknowledges and accepts that its representations on disclosure during consultation may not be determinative and that the decision whether to disclose Information in order to comply with the Act or the Regulations is a matter in which the Authority shall exercise its own discretion, subject always to the provisions of the Act or the Regulations. For the avoidance of doubt, nothing in this Condition shall affect the Contractor's rights at law.

11. Nothing in this Condition shall affect the parties' obligations of confidentiality where information is disclosed orally in confidence.

Annex D

Methods of Encryption for Removable Storage Media and Devices

The products detailed in the table below are extracts from Industry Security Notice 2020/07; please note ISNs are regularly updated and the latest version should always be consulted. The methods of encryption are either Approved, indicating evaluation and certification by the National Cyber Security Centre (NCSC), or Acceptable, indicating evaluation by the Technical Authorities of another nation and/or approval by the former MOD/Industry Defence Infosec Product Cooperation Group (DIPCOG); Dstl's preferred options are highlighted.

The use of optical media for above OFFICIAL purposes must only be selected when it is completely infeasible to use an approved hardware encryption product. The encryption products detailed are appropriate for External Storage Devices (ESD) and Optical Storage Devices (e.g. CDs and DVDs).

Where passwords are used in association with encryption these should be complex and long; a minimum of 16 characters comprising UPPER and lower case, special characters and numbers. Passwords are to be sent via a different medium; the preferred method is email via RLI if available, otherwise posted as a separate item.

Once encrypted, the MOD/Dstl material on the Removable Storage Media and Devices (RSMD) must still be protected in accordance with all the relevant control measures for the classification; the application of encryption does not reduce the classification of the information and therefore all control measures are to be applied, e.g. method of transmission, storage, etc.

Methods of Encryption for External Storage Devices (ESD)

Encryption Product	Highest Classification	Comments
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

Methods of Encryption for Optical Storage Media (OSM), e.g. CDs and DVDs

The use of encrypted optical storage media for above OFFICIAL purposes **must only** be selected when it is completely infeasible to use an approved hardware encryption product.

[redacted]		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]