Click or tap here to enter Company Name

For the personal attention of: Click or tap here to enter name of Security Controller.

Click or tap here to enter company postal address

Our Ref: ITT RQ0000008326

Your Ref: Click or tap here to enter text.

Date: 16/05/2022

Security Aspects Letter (SAL) for an Invitation to Tender (ITT) for a Contract Involving Information Classified OFFICIAL and OFFICIAL-SENSITIVE, but not above, to Overseas Firms

Dear Sirs,

TENDER NUMBER AND SUBJECT: RQ0000008326 for the procurement of passive and/or active anti-vibration systems

DATE OF TENDER: 16/05/2022 (to be inserted by Commercial staff)

DESCRIPTION: Procurement of passive and/or active anti-vibration systems for vibration sensitive equipment at Dstl Porton Down

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 classified material, including UK OFFICIAL-SENSITIVE for the purposes of DEFCON 660, are specified below. These aspects must be fully safeguarded. The Security Conditions at Appendix 1 to Annex A outline the minimum measures required to safeguard UK OFFICIAL-SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
Survey data	OFFICIAL

Tender document details including the background and requirement information	OFFICIAL
Room dimension and layout	OFFICIAL

(add more rows as required)

3. You are required to provide at least the same protection to this information as you are obliged to give information of equal security grading entrusted to you by your own government. Your attention is drawn to the requirements of the Security Conditions at Appendix 1 to Annex A. you should take all reasonable steps to make sure that all individuals employed on any work in connection with the ITT that have access to classified information and assets are aware of the protective requirements and that such requirements will continue to apply should the ITT be unsuccessful.
4. You are requested to acknowledge receipt of this letter, in writing, confirming that:
    a) The definition of the classified aspects of the referenced ITT has been brought to the attention of the person directly responsible for the security of the classified information.
    b) The definition is fully understood.
    c) The requirement and obligations set out herein and in any subsequent contractual document if so awarded can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations.

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

    Click or tap here to enter text.
5. If you have any difficulty in either 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 classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer in accordance with DEFCON 76.
8. Where there is a requirement to forward information relating to the tender to Dstl using removable computer media (e.g. CD, DVD, USB device) such media must be encrypted. At classifications of OFFICIAL and OFFICIAL-SENSITIVE, the media is to be encrypted using Ivanti Device Control (Secure Volume Browser)

https://www.ivanti.com/products/device-control Previously known as Sanctuary, Lumension and Heat. Ivanti Device Control 4.3.2 and upwards, choose the newest version available. . See Annex B for additional details on appropriate encryption products.

9. 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 destroyed appropriately according to their classification

Yours sincerely

Craig Delaney

Commercial Manager

Copy via email to:

- The Demander
- ISAC-group@mod.gov.uk (MULTIUSER)
- SPODSR-IIPCSy@mod.gov.uk (MULTIUSER)
- ISS Des-DAIS-SRAAcc4-IA

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 the 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 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. All 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 and handle such documents without being specifically named in the distribution list.
4. Recipients of LIMCIRC documents must not circulate the document further without the explicit approval of 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’.

Appendix 1 to Annex A

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: SPODSR-IIPCSy@mod.gov.uk).

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:

- https://www.gov.uk/government/publications/industry-security-notices-isns.
- https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138
- https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down

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:

    https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.

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:

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

    Details of the CPA scheme are available at:

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

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:

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

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.

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

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

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: defencewarp@modnet.rli.uk (MULTIUSER)

Email: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions))

Telephone (Office Hours): +44 (0) 30 6770 2185

JSyCC Out of Hours/Duty Officer Phone: +44 (0) 7768 558863

Mail: JSyCC Defence Industry WARP, X007 Bazalgette Pavilion, RAF Wyton, HUNTINGDON, Cambridgeshire, PE28 2EA.

30. Reporting instructions for any security incidents involving MOD classified material can be found in Industry Security Notice 2017/03 as may be subsequently updated at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651683/ISN_2017-03_-_Reporting_of_Security_Incidents.pdf

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:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf

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:

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

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 B

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
iStorage diskAshur DT2 HDD	OFFICIAL (inc. OFFICIAL-SENSITIVE)	Approved https://www.ncsc.gov.uk/products/istorage-diskashur-dt2-hdd
iStorage diskAshur PRO2 HDD/SDD	OFFICIAL (inc. OFFICIAL-SENSITIVE)	Approved https://www.ncsc.gov.uk/products/istorage-diskashur-pro2-hddssd
SDMS Mk III AESLock Encrypted USB Stick	OFFICIAL (inc. OFFICIAL-SENSITIVE)	Acceptable/Endorsed Colour-coded BUFF http://sdms.uk.com/storage-devices/
ViaSat Eclypt 300 Freedom Baseline	OFFICIAL (inc. OFFICIAL-SENSITIVE)	Approved https://www.ncsc.gov.uk/products/viasat-uk-eclypt-300baseline
ViaSat Eclypt 400 Freedom Baseline Plus	OFFICIAL (inc. OFFICIAL-SENSITIVE)	Approved https://www.ncsc.gov.uk/products/viasat-uk-eclypt-400baseline-plus
ViaSat Eclypt 600 Freedom Enhanced	TOP SECRET	Approved https://www.ncsc.gov.uk/products/viasat-uk-eclypt-600enhanced

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.

Encryption Product	Highest Classification	Comments
Ivanti Device Control (Secure Volume Browser)	SECRET	Acceptable/Endorsed https://www.ivanti.com/products/device-control Previously known as Sanctuary, Lumension and Heat. Ivanti Device Control 4.3.2 and upwards, choose the newest version available.
WinZip (AES 256)	SECRET	Acceptable/Endorsed WinZip 10 and upwards; choose the newest version available. Data must be 'double zipped', i.e. a zip file placed within an encrypted zip file to ensure that file names are not readable without a password. Standard/Legacy/ZipCrypto are not to be used under any circumstances.