EUSPA/OP/17/23

HADG Infrastructure for HAS Phase 2

ANNEX I.J to Invitation To Tender

'Security Aspects Letter'

Table of Contents

1. Introduction

This document represents the security aspects letter ('SAL') issued by the European Union Agency for the Space Programme (hereinafter referred to as 'EUSPA' or 'the contracting authority'). It shall form an integral part of the classified contract or subcontract referred to on the cover page and of any subsequent specific contract under which European Union classified information ('EUCI') may be accessed, handled or created (hereinafter referred as the 'contract' and 'handling').

This document sets out the specific requirements for the performance of the tasks defined for the contract requiring handling of EUCI. In accordance with the Regulation [RD-1] which stipulates that the contracting authority shall comply with the security requirements of the Programme components and contribute to the protection of the essential security interests of the Union and its Member States, the contracting authority is required to protect EUCI in accordance with Commission Decision (EU, Euratom) 2015/444 [RD-2] and its implementing rules [RD-4 to 6] and in accordance with the Decision of the Administrative Board on the security rules for protection of EUCI [RD-3]., This SAL applies to any legal entity involved in contractual or pre-contractual activities through this contract and the contractor shall ensure that this SAL forms integral part of any subcontract.

Where the term "contractor" is used in this document, the applicable provisions shall apply to the prime contractor (including all members of the consortium) and subcontractors in respect to those subcontracts for which access to the EUCI is required in order to perform the tasks foreseen in the contract.

Where the SAL refers to national laws, regulations and/or requirements and if the contractor is an economic operator established by an international organisation, equivalent regulations, rules and requirements of that international organisation shall apply.

A list of all the elements in the contract which are classified or to be classified in the course of the performance of the contract, the rules for so doing and the specification of the applicable security classification levels are contained in the security classification guide ('SCG'). General principles of SCG describing the classified elements of the contract and subsequent specific contracts are laid down in Appendix 1. The project specific SCG related to this contract [AD-2] will be shared upon submission of a non-disclosure undertaking ('NDU') by the economic operator, if applicable to the contract.

The guidance on the interpretation and application of the rules set out in Commission Decision 2015/444 [RD-2] and its implementing rules [RD-4 to 6] and the Decision of the Administrative Board on the security rules for protecting EUCI [RD-3], and in particular Chapters 6 of RD-2 and RD-3 is provided by the documents referred under AD-1 and AD-2 applicable to the contract. The definitions set out in AD-1 shall be applicable to this SAL.

The contractor's security authority ('NSA/DSA') is responsible for ensuring that the contractor under its jurisdiction complies with the applicable security regulations for the protection of EUCI.

Where the contract requires the generation, handling or storage of assets or information marked CRYPTO or CCI, the contractor's Crypto Authority ('CA') shall be responsible for issuing the crypto account required to hold, manage and operate cryptographic material.

Non-compliance with the requirements of the SAL may constitute sufficient grounds for termination of the contract under the conditions stipulated therein.

Amendments to the requirements of the SAL, made by the EUSPA in accordance with law, relevant programme security instruction ('PSI') or the relevant security classification guide ('SCG'), shall become integral part of the contract. Such additions and amendments shall be notified by EUSPA to the contractor and shall become effective upon such notification.

In accordance with Article 42, 2 (b), (c) of Commission Decision 2015/444 [RD-2] and Article 39, 2 (b), (c) of Decision of the Administrative Board on the security rules for protection of EUCI [RD-3], the overall level of security classification of the contract is up to level CONFIDENTIEL UE/EU CONFIDENTIAL, as the contractor's personnel may have access to secured areas accredited at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or handle information or material classified up to CONFIDENTIEL UE/EU CONFIDENTIAL.

2. General Conditions

- [REQ 2.1] Contractors shall be subject to all the obligations laid down in Commission Decision 2015/444 [RD-2] and its implementing rules referred under RD-4 to 6 and in Decision of the Administrative Board on the security rules for protecting EUCI [RD-3]. The contractor shall handle and protect EUCI provided or created under the contract in accordance with the relevant PSI [AD-1] and the supplementary provisions referred to in this SAL, AD-6, AD-7, AD-8 and other subsequent subject matter provisions emanating from the Contracting Authority. The Contractor shall comply with any additional instructions issued by the Contractor's competent Security Authority.

- [REQ 2.2] Classified information created throughout the lifecycle of classified contract must be marked as EUCI at security classification level, as determined in the relevant SCG [AD-2] in accordance with Article 3 of RD-2 and Articles 8 of its implementing rules listed under RD-5 and RD-6 and Article 3 of RD-3. Deviation from the security classification level stipulated by the relevant SCG [AD-2] is permissible only with the written authorisation of the contracting authority.

- [REQ 2.3] The rights pertaining to the originator of any EUCI created and handled for the performance of the classified contract are exercised by the EUSPA, as the contracting authority.

- [REQ 2.4] Without the written consent of the contracting authority, the contractor or subcontractor must not make use of any information or material furnished by the contracting authority or produced on behalf of that authority for any purpose other than that of the contract.

- [REQ 2.5] In case information related to the Galileo Public Regulated Service, as identified in the specific Security Classification Guide [AD-2], shall be handled in performing the contract, contractors and subcontractors are subject to the specific requirements specified in relevant PSI [AD-1] and its Annexes. When handling of classified PRS information is required, the Contractor shall demonstrate to the contracting authority of being authorised for this purpose by the Competent PRS Authority (CPA) of the Member State in which the contractor is established and by the

Security Accreditation Board for the Space Programme. Such authorisations shall indicate the classification level up to that the contractor and sub-contractors can handle and the corresponding PRS authorisation category.

3. Access to EUCI

- [REQ 3.1] EUCI released to the contractor or created throughout the lifecycle of classified contract shall not be disclosed to any other entity or person (including subcontractors) other than those of its personnel without prior explicit written approval of the contracting authority.

- [REQ 3.2] The personnel of a contractor or subcontractor, for the performance of the classified contract or sub-contract, may only be granted access to EUCI if:

    - it has been established that they have a need-to-know in relation to the performance of the contract,
    - they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regards to protecting such information by the Contractor's Security Officer on the applicable security rules for protecting EUCI, and on the consequences of any compromise or breach of security of such information,
    - for information classified CONFIDENTIEL UE/EU CONFIDENTIAL level or SECRET UE/EU SECRET, they have been granted a Personnel Security Clearance (PSC) within the meaning of Decision 2015/444 [RD-2] and Decision of the Administrative Board on the security rules for protection of EUCI [RD-3], at the relevant level, by the respective NSA/DSA or any other competent security authority.

- [REQ 3.3] All contractors and sub-contractors participating in the contract requiring creation or access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET at the contractor's premises shall ensure that a valid facility security clearance (FSC) at the appropriate level exists for the premises. This FSC is being granted by the respective NSA/DSA or any other competent security authority of the contractor. Where such an FSC necessary for the execution of the contract is withdrawn, the contractor with whom the contracting authority signed the contract, shall immediately inform the contracting authority.

- [REQ 3.4] The Contractor is responsible for knowing the security certification and/or accreditation status of all consortium members (if any) and sub-contractors involved in the Contract and for reporting any changes to the EUSPA Security Authority.

- [REQ 3.5] After the end of the contract, the contractor or subcontractor must return any EUCI it holds to the contracting authority as soon as possible. Where practicable, the contractor or subcontractor may destroy EUCI instead of returning it. This must be done in accordance with the national laws and regulations of the country where the contractor is based, with the prior agreement of the

EUSPA Security Authority, and under the latter's instruction. EUCI must be destroyed in such a way that it cannot be reconstructed, either wholly or in part.

- [REQ 3.6] Where the contractor or subcontractor is authorised to retain EUCI after termination or conclusion of the contract, the EUCI must continue to be protected in accordance with RD-2, and with its implementing rules referred under RD-4 to 6, and in accordance with RD-3.

4. Access and handling of EUCI at RESTREINT UE/EU RESTRICTED level

- [REQ 4.1] A personnel security clearance (PSC) is not required for compliance with the contract. However, information or material classified RESTREINT UE/EU RESTRICTED must be accessible only to contractor personnel who require such information to perform the contract (need-to-know principle), who have been briefed by the contractor's security officer on their responsibilities and on the consequences of any compromise or breach of security of such information, and who have acknowledged in writing the consequences of a failure to protect EUCI.

- [REQ 4.2] Except where the contracting authority has given its written consent, the contractor or subcontractor must not provide access to information or material classified RESTREINT UE/EU RESTRICTED to any entity or person other than those of its personnel who have a need-to-know.

- [REQ 4.3] Information or material classified RESTREINT UE/EU RESTRICTED must be stored in locked office furniture when not in use. When in transit, documents must be carried inside an opaque envelope. The documents must not leave the possession of the bearer and they must not be opened en route.

- [REQ 4.4] The contractor or subcontractor may transmit documents classified RESTREINT UE/EU RESTRICTED to the contracting authority using commercial courier companies, postal services, hand carriage or electronic means. To this end, the contractor or subcontractor must follow the relevant Programme (or project) Security Instruction (PSI) [AD-1] issued by the contracting authority and/or the relevant implementing rules on industrial security with regard to classified procurement contracts [RD-4].

- [REQ 4.5] When no longer required, documents classified RESTREINT UE/EU RESTRICTED must be destroyed in such a way that they cannot be reconstructed, either wholly or in part.

- [REQ 4.6] Unless stated differently in the relevant PSI [AD-1], the security accreditation of contractor CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the security officer of a contractor if national laws and regulations so permit. Where accreditation is thus delegated, the NSAs/DSAs/SAAs retain responsibility for protecting any RESTREINT UE/EU RESTRICTED information that is handled by the contractor and the right to inspect the security measures taken by the contractor. In addition, the contractor shall

provide the contracting authority and, where required by national laws and regulations, the competent national SAA with a statement of compliance certifying that the contractor CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level. The minimum requirements for CIS handling information classified RESTREINT UE/EU RESTRICTED are laid down in Appendix 2 to this SAL.

5. Marking of EUCI

- [REQ 5.1] The contractor shall mark EUCI at security classification level, as determined in the relevant SCG [AD-2] in accordance with Article 3 of Decision 2015/444 [RD-2] and Articles 8 of its implementing rules listed under RD-5 and RD-6, and in accordance with Article 3 of the Annex to the Decision of the Administrative Board on the security rules for protecting EUCI [RD-3].

- [REQ 5.2] The contractor or subcontractor must maintain the security classification markings of classified information created or provided throughout the lifecycle of classified contract and must not declassify information without written consent from the contracting authority.

6. Electronic handling

- [REQ 6.1] Any electronic handling, processing and transmission of EUCI must abide by the provisions laid down in Chapters 5 and 6 of RD-2 and Chapter 5 and 6 of RD-3. These include, inter alia, the requirement that communication and information systems owned by the contractor and used to handle EUCI for the purpose of the contract (hereinafter 'contractor CIS') must be subject to accreditation;[1] that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 36(4) of RD-2 and Article 34(4) of RD-3, and that TEMPEST measures must be implemented in accordance with Article 36(6) of RD-2 and Article 34(6) of RD-3. The minimum requirements for CIS handling information classified RESTREINT UE/EU RESTRICTED are laid down in Appendix 2 to this SAL.

- [REQ 6.2] EUCI shall only be encrypted using cryptographic products approved by the EU Council. Where products are to be used for communication with the contracting authority, the product shall be agreed with the EUSPA Security Authority. The system to be used for exchange of information marked RESTREINT UE/EU RESTRICTED or equivalent with EUSPA is the EUSPA SPIDER Network w/ Filkrypto system. For such purpose, the SPIDER Networks CONOPS [AD-3], SPIDER Network w/ Filkrypto SECOPS [AD-4] and SPIDER Networks w/ Filkrypto Key

[1] The party undertaking the accreditation will have to provide the contracting authority with a statement of compliance, through the EUSPA Security Authority, and in coordination with the relevant national security accreditation authority (SAA).

Management Plan [AD-5] shall be applied. Filkrypto software is not a Customer Furnished Item (CFI).

Internal exchanges of EUCI RESTREINT UE/EU RESTRICTED between only the contractor and its subcontractors shall be performed using:
- a communication information system (CIS) accredited by the relevant national security authorities;
- or using SPIDER Networks (possibility to establish internal[2] communities).

- [REQ 6.3] The security accreditation of contractor CIS handling EUCI and any interconnection thereof shall be conducted in accordance with the applicable rules set by the contractor's security authorities (NSA/DSA/SAA). In addition, the contractor shall provide to the contracting authority evidence that the contractor CIS and respective interconnections have been accredited for handling EUCI at required level.

- [REQ 6.4] Where CIS is to be used to handle EUCI, the contractor shall ensure that security operating procedures (SecOps) describing how to maintain a secure storage, transport and operating environment for the CIS exist and are available to their personnel for all CIS used to handle EUCI under this contract. Where there is no explicit SecOps provided upon acquisition of the CIS, and where no SecOps exist in documentation provided with the CIS, the contractor shall create SecOps specifying the conditions for use of the CIS under the contract.

- [REQ 6.5] All persons involved in contractual activities that are required to access CIS for handling EUCI shall do so in accordance with the security operating procedures (SecOps) applicable to that CIS, whether provided with the CIS upon acquisition or developed for the CIS by the contractor.

7. Security incident management

- [REQ 7.1] The contractor must investigate all security breaches related to EUCI and report them to the contracting authority as soon as is practicable. The contractor or subcontractor must immediately report to its responsible national security authority (NSA) or to the designated security authority (DSA), and, where national laws and regulations so permit, to the EUSPA security authority, all cases in which it is known or there is a reason to suspect that EUCI provided or created pursuant to the contract has been lost or disclosed to unauthorised persons.

- [REQ 7.2] The contractor or subcontractor shall have business contingency plans (BCP) to protect any EUCI handled throughout the lifecycle of classified contract in emergency situations and shall put in place preventive and recovery measures to minimise the impact of incidents associated with

[2] Memberships of Internal communities are defined by the contractor while associated key material is created and distributed by EUSPA.

the handling and storage of EUCI. The contractor or subcontractor must inform the contracting authority of its BCP.

8. Conditions under which the contractors may subcontract

- [REQ 8.1] The contractor must obtain permission from the contracting authority, before subcontracting any part of a classified contract.

- [REQ 8.2] No subcontract may be awarded to a company registered in a non-EU Member State or to an entity belonging to an international organisation, if that non-EU Member State or international organisation has not concluded a security of information agreement with the EU or a security administrative arrangement with the contracting authority.

- [REQ 8.3] Where the contractor has let a subcontract, the security provisions of the contract shall apply mutatis mutandis to the subcontractor(s) and its (their) personnel. In such a case, it is the contractor's responsibility to ensure that all subcontractors apply these principles to their own subcontracting arrangements. To ensure appropriate security oversight, the contractor's and subcontractor's NSAs/DSAs shall be notified of the letting of all related classified subcontracts at the levels of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET. Where appropriate, the contractor's and subcontractor's NSAs/DSAs shall be provided with a copy of the subcontract-specific security provisions. NSAs/DSAs requiring notification about the security provisions of classified contracts at RESTREINT UE/EU RESTRICTED level are listed in the annex to the Commission's implementing rules on industrial security with regard to classified procurement contracts [RD-4].

- [REQ 8.4] The contractor may not release any EUCI to a subcontractor without the prior written approval of the contracting authority. If EUCI to subcontractors is to be sent frequently or as a matter of routine, then the contracting authority may give its approval for a specified length of time (e.g. 12 months) or for the duration of the subcontract.

9. Security Organisation

- [REQ 9.1] The contractor shall declare to the contracting authority the interface to its security organisation via nominated point(s) of contact, in each case specifying the name, post, address, telephone number and email address of the point(s) of contact.

- [REQ 9.2] The contractor shall ensure that at least one of their points of contact be the local security officer (‘LSO’) who is able to act as a liaison and co-operation contact for the contracting authority LSO regarding security matters pertaining to the contract.

- [REQ 9.3] In case of any change to the security organisation which is relevant to the contract and is established by the contractor throughout the term of applicability of the contract, the contractor

shall immediately update the information and inform the contracting authority LSO in writing about all relevant details of the changes within 30 (thirty) days of their occurrence.

10. Visits and access to EUSPA classified premises

- [REQ 10.1] Where access to contracting authority premises is required for contractual activities, contractors and their personnel shall comply with the contracting authority internal security rules [RD-3] and regulations, procedures and shall follow any instructions given by the contracting authority LSO. Contractors' personnel will be briefed accordingly by the contracting authority LSO. They shall grant their full co-operation to prevent and report any (security) incident they detect.

- [REQ 10.2] Visits involving access or potential access to EU classified information shall be arranged in accordance with the relevant PSI [AD-1].

- [REQ 10.3] The facility hosting the visit must ensure that records are kept of all visitors. These must include their names, the organisation they represent, the date of expiry of the PSC (if applicable), the date of the visit and the name(s) of the person(s) visited. Without prejudice to European Data-Protection Rules, such records are to be retained for a period of no less than five years or in accordance with national rules and regulations, as appropriate.

11. Assessment visits

- [REQ 11.1] The EUSPA Security Authority may, in cooperation with the relevant NSA/DSA, conduct visits to contractors' or subcontractors' facilities to check that the security requirements for handling EUCI are being complied with.

12. Applicable and reference documents

12.1 Applicable documents

AD-1 Relevant programme security instruction[3] ('PSI') in its latest version;

AD-2 Tailored HAS Phase 2 Security Classification Guide, ref EUSPA-SEC-SRS-SCG-R01335-RUE, version 1.1;

AD-3 SPIDER Networks CONOPS, ref. GSA-SEC-CA-UM-A03997, in its latest version;

[3] For Galileo and EGNOS the applicable PSI is European GNSS PSI v.4.1, for GOVSATCOM and IRIS[2] activities the applicable PSI is GOVSATCOM PSI, ref. Ares(2022)8649697, for EuroQCI activities the applicable PSI is EuroQCI PSI, ref. Ares(2023)1913047. Not applicable to COPERNICUS and SST.

AD-4 SPIDER Networks w/ Filkrypto SECOPS, ref. GSA-SEC-CA-UM-A01718, in its latest version;

AD-5 SPIDER Networks w/ Filkrypto Key Management Plan ref. GSA-SEC-CA-UM-A01392, in its latest version;

AD-6 Guidelines for deliveries of EU classified information level RESTREINT UE/EU RESTRICTED, ref. EUSPA-SEC-CSO-PRC-A21678 in its latest version;

AD-7 Guidelines for deliveries of EU classified information level CONFIDENTIEL UE/EU CONFIDENTIAL and above, ref. EUSPA-SEC-CSO-PRC-A15666 in its latest version;

AD-8 EUSPA Delivery rules and procedure, ref. EUSPA-PCEDQ-CADM-PRC-A10070 in its latest version.

12.2 Reference documents

RD-1 Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU;

RD-2 Commission Decision No 2015/444 of 13 March 2015 on the security rules on the protection of EUCI;

RD-3 Decision No. EUSPA-AB-08-23-01-09 of the Administrative Board of 26 January 2023 on the security rules for protecting EU Classified Information, ref. EUSPA-SEC-AB-DEC-A22114;

RD-4 Commission Decision (EU, Euratom) 2019/1963 of 17 October 2019 laying down implementing rules on industrial security with regard to classified procurement contracts;

RD-5 Commission Decision (EU, Euratom) 2019/1961 of 17 October 2019 laying down implementing rules on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information;

RD-6 Commission Decision (EU, Euratom) 2019/1962 of 17 October 2019 laying down implementing rules on implementing rules for handling RESTREINT UE/EU RESTRICTED information;

RD-7 Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on the rules of access to the public regulated service provided by the global navigation satellite system established under the Galileo Programme.

Appendix 1 – General principles of security classification guide

1. The information created by the contractor throughout the lifecycle of classified contract that requires classification shall be
    a. considered as EU classified information for which the rights incumbent on the originator are exercised by the contracting authority and
    b. classified and marked in accordance with the relevant security classification guide ('SCG') issued with the contract, using only the classification, annotation and caveat markings detailed in the relevant PSI [AD-1].
    c. Specific instructions[4] for marking classified PRS information are set out in the relevant PSI [AD-1] and its annexes.

2. If the contractor intends to use a marking that differs from the marking specified or implied in the relevant SCG [AD-2], it shall provide a written justification for the intended marking, which shall be reviewed and approved by the EUSPA Security Authority.

3. While awaiting for the response of the contracting authority, the information shall either not be produced in recorded form or shall be classified according to the specification assigned in the SCG and all parties shall handle it accordingly until the contracting authority has decided on the final classification level to be assigned and communicated it in writing to the contractor. The SCG shall then be updated by the contracting authority to reflect the new classification scenario and reissued to the contractor.

4. In instances where the contractor encounters a classified asset with an EU classification marking that differs from the programme marking scheme defined in the relevant PSI [AD-1], the information and assets shall be handled in accordance with the relevant PSI [AD-1] and, if possible, the marking shall be changed accordingly[5].

[4] Where such instructions are not yet provided in [AD1] and its Annexes or in a working document of the European Commission, classified PRS Information documented by the Contractor or any subcontractor shall be clearly marked for informational purposes only as such by including the text "This document contains classified PRS information." on each page. It shall be noted that these substitute markings have no legal meaning as security markings and are to be used only if the PSI provides no guidance. Should such markings be encountered in instances where the PSI provides instructions on PRS marking then the PSI take precedence, the legacy markings should be replaced and the assets/information shall be protected as if marked by the applicable PSI markings.

[5] Such instances may arise where revisions of AD-1 result in unsupported markings assigned to existing information and assets, or where the legacy marking for information or assets needs to be revised/updated. In all instances where ambiguity exists, the PSI [AD-1] provides clarification on handling legacy markings.

Appendix 2 - Minimum requirements for protection of EUCI in electronic form at RESTREINT UE/EU RESTRICTED level handled in the contractor's CIS

General

1. The contractor must be responsible for ensuring that the protection of RESTREINT UE/EU RESTRICTED information complies with the minimum security requirements as laid down in this security clause and with any other additional requirements advised by the contracting authority or, if applicable, by the national security authority ('NSA') or designated security authority ('DSA')

2. It is the contractor's responsibility to implement the security requirements identified in this document.

3. For the purpose of this document, a communication and information system (CIS) covers all equipment used to handle, store and transmit EUCI, including workstations, printers, copiers, fax machines, servers, network management systems, network controllers and communications controllers, laptops, notebooks, tablet PCs, smart phones and removable storage devices such as USB-sticks, CDs, SD-cards, etc.

4. Special equipment, such as cryptographic products, must be protected in accordance with its dedicated security operating procedures (SecOps).

5. Contractors must establish a structure responsible for the security management of the CIS handling information classified RESTREINT UE/EU RESTRICTED and appoint a security officer responsible for the facility concerned.

6. The use of IT solutions (hardware, software or services) privately owned by contractor staff for storing or processing RESTREINT UE/EU RESTRICTED information is not permitted.

7. Accreditation of the contractor's CIS handling information classified RESTREINT UE/EU RESTRICTED must be approved by the security accreditation authority (SAA) of the Member State concerned or delegated to the contractor's security officer as permitted by national laws and regulations.

8. Only information classified RESTREINT UE/EU RESTRICTED that is encrypted using approved cryptographic products may be handled, stored or transmitted (by wired or wireless means) as any other

unclassified information under the contract. Such cryptographic products must be approved by the EU or a Member State.

9. External facilities involved in maintenance/repair work must be contractually obliged to comply with the applicable provisions for handling of information classified RESTREINT UE/EU RESTRICTED, as set out in this document.

10. At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor must provide evidence of compliance with the contract security clause. If an audit and inspection of the contractor's processes and facilities are also requested, to ensure compliance with these requirements, contractors shall permit representatives of the contracting authority, the NSA/DSA/SAA, or the relevant EU security authority to conduct such an audit and inspection.

Physical security

11. Areas in which CIS are used to display, store, process or transmit RESTREINT UE/EU RESTRICTED information or areas housing servers, network management systems, network controllers and communications controllers for such CIS should be established as separate and controlled areas with an appropriate access control system. Access to these separate and controlled areas should be restricted to individuals with specific authorisation. Without prejudice to paragraph 8, equipment as described in paragraph 3 must be stored in such separate and controlled areas.

12. Security mechanisms and/or procedures must be implemented to regulate the introduction or connection of removable computer storage media (such as USBs, mass storage devices or CD-RWs) to components on the CIS.

Access to CIS

13. Access to a contractor's CIS handling EUCI is allowed on a basis of strict need-to-know and authorisation of personnel.

14. All CIS must have up-to-date lists of authorised users. All users must be authenticated at the start of each processing session.

15. Passwords, which are part of most identification and authentication security measures, must be at least nine characters long and must include numeric and 'special' characters (if permitted by the system) as

well as alphabetic characters. Passwords must be changed at least every 180 days. They must be changed as soon as possible if they have been compromised or disclosed to an unauthorised person, or if such compromise or disclosure is suspected.

16. All CIS must have internal access controls to prevent unauthorised users from accessing or modifying information classified RESTREINT UE/EU RESTRICTED and from modifying system and security controls. Users are to be automatically logged off the CIS if their terminals have been inactive for some predetermined period of time, or the CIS must activate a password-protected screen saver after 15 minutes of inactivity.

17. Each user of the CIS is allocated a unique user account and ID. User accounts must be automatically locked once at least five successive incorrect login attempts have been made.

18. All users of the CIS must be made aware of their responsibilities and the procedures to be followed to protect information classified RESTREINT UE/EU RESTRICTED on the CIS. The responsibilities and procedures to be followed must be documented and acknowledged by users in writing.

19. SecOps must be available for the users and administrators and must include descriptions of security roles and associated list of tasks, instructions and plans.

Accounting, audit and incident response

20. Any access to the CIS must be logged.

21. The following events must be recorded:
    a. all attempts to log on, whether successful or failed;
    b. logging off (including being timed out, where applicable);
    c. creation, deletion or alteration of access rights and privileges;
    d. creation, deletion or alteration of passwords.
22. For all of the events listed above the following information must be communicated as a minimum:
    a. type of event;
    b. user ID;
    c. date and time;
    d. device ID.

23. The accounting records should provide help to a security officer to examine the potential security incidents. They can also be used to support any legal investigations in the event of a security incident. All security records should be regularly checked to identify potential security incidents. The accounting records must be protected from unauthorised deletion or modification.

24. The contractor must have an established response strategy to deal with security incidents. Users and administrators must be instructed on how to respond to incidents, how to report them and what to do in the event of emergency.

25. The compromise or suspected compromise of information classified RESTREINT UE/EU RESTRICTED must be reported to the contracting authority. The report must contain a description of the information involved and a description of the circumstances of the compromise or suspected compromise. The contractor or subcontractor must immediately report to its responsible national security authority (NSA) or to the designated security authority (DSA), and, where national laws and regulations so permit, to the EUSPA security authority, all cases in which it is known or there is reason to suspect that EUCI provided or created pursuant to the contract has been lost or disclosed to unauthorised persons. All users of the CIS must be made aware of how to report any actual or suspected security incident to the security officer.

Networking and interconnection

26. When a contractor CIS that handles information classified RESTREINT UE/EU RESTRICTED is interconnected to a CIS that is not accredited, this significantly increases the threat to both the security of the CIS and the RESTREINT UE/EU RESTRICTED information that is handled by that CIS. This includes the internet and other public or private CIS, such as other CIS owned by the contractor or subcontractor. In this case, the contractor must perform a risk assessment to identify the additional security requirements that need to be implemented as part of the security accreditation process. The contractor shall provide to the contracting authority, and where required by national laws and regulations, the competent SAA, a statement of compliance certifying that the contractor CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.

27. Remote access from other systems to LAN services (e.g. remote access to email and remote SYSTEM support) is prohibited unless special security measures are implemented and agreed by the contracting authority, and where required by national laws and regulations, approved by the competent SAA.

Configuration management

28. A detailed hardware and software configuration, as reflected in the accreditation/approval documentation (including system and network diagrams) must be available and regularly maintained.
29. The contractor's security officer must conduct configuration checks on hardware and software to ensure that no unauthorised hardware or software has been introduced.

30. Changes to the contractor CIS configuration must be assessed for their security implications and must be approved by the security officer, and where required by national laws and regulations, the SAA.

31. The system must be scanned for any security vulnerabilities at least once a quarter. Software to detect malware must be installed and kept up-to-date. If possible, such software should have a national or recognised international approval, otherwise it should be a widely accepted industry standard.

32. The contractor must develop a business continuity plan. Back-up procedures must be established to address the following:
    a. frequency of back-ups;
    b. storage requirements on-site (fireproof containers) or off-site;
    c. control of authorised access to back-up copies.

Sanitisation and destruction

33. For CIS or data storage media that have at any time held RESTREINT UE/EU RESTRICTED information the following sanitisation must be performed to the entire system or to storage media before its disposal:
    a. flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must be overwritten at least three times and then verified to ensure that the original content cannot be recovered, or be deleted using approved deletion software;
    b. magnetic media (e.g. hard disks) must be overwritten or degaussed;
    c. optical media (e.g. CDs and DVDs) must be shredded or disintegrated;
    d. for any other storage media, the contracting authority or, if appropriate, the NSA/DSA/SAA should be consulted on the security requirements to be met.

34. Information classified RESTREINT UE/EU RESTRICTED must be sanitised on any data storage media before it is given to any entity that is not authorised to access information classified RESTREINT UE/EU RESTRICTED (e.g. for maintenance work).