ESA/REG/004
Paris, 18 January 2012
(Original: English)

REGULATIONS OF THE EUROPEAN SPACE AGENCY

Security Regulations

The attached Security Regulations of the European Space Agency apply to the Agency, its Member States, its staff and, under certain conditions, to its contracting personnel and to its contractors.

These Security regulations have been adopted by ESA Council at its 226th meeting held on 14-15 December 2011 and shall enter into force on 1st January 2012.

The attached Security Regulations shall supersede, as of 1st January 2012, the ESA Security Regulations Part I (ESA/C/R/CLXI/Rules 1 (Final)) and Part II (ESA/C/CLXVI/Rules 1 (Final)) which were adopted by ESA Council on 11 December 2002 and 12 June 2003, respectively.

The ESA Council authorised public release of these Security Regulations on the occasion of their adoption at the same 226th meeting.

- This page is left intentionally blank -

ESA SECURITY REGULATIONS

TABLE OF CONTENTS

SECTION I - GENERAL PRINCIPLES FOR THE PROTECTION OF CLASSIFIED INFORMATION

1. Pursuant to the ESA Security Agreement[1], and with a view to ensuring a common degree of protection for Classified Information, these Security Regulations lay down the basic security principles and minimum standards to be applied by the European Space Agency (hereinafter referred to as "ESA") and by the ESA Member States, in accordance with their respective laws and regulations insofar as they provide an equivalent level of protection.

2. For the purpose of these Regulations, Classified Information means any information, document or material designated with a security classification marking which is generated and submitted in whatever form by ESA to a Member State, or by a Member State to ESA, or to another Member State in support of an ESA programme, project or contract and whose unauthorised disclosure could damage the interests of ESA or of one or more of its Member States. As necessary in these Regulations, the Classified Information which is generated by ESA or by its Member States in the framework of an ESA Programme shall be designated as "ESA Classified Information" and shall respond to the Classification Levels and markings defined in Section IV paragraph 2 of these Regulations.

3. The protection of Classified Information responds to the following objectives:

   a) to safeguard such information from security breaches and compromise, through the provisions described in Sections III, IV , V and X;

   b) to safeguard installations holding such information from unauthorised access, sabotage and malicious wilful damage, as described in Section III;

   c) to safeguard such information handled in Communications and Information Systems and their associated networks, against threats to its integrity and availability, as described in Section VI;

   d) in the event of an emergency situation, to assess the damage caused, limit its consequences and adopt the necessary remedial measures, as described in Section VIII;

   e) to implement the appropriate security measures in the framework of ESA industrial activities, including the pre-negotiation, negotiation and placing of ESA classified contracts as described in Section VII.

   f) to lay down the requirements for exchanging such information with third States and International Organisations through Security Agreements and memoranda of understanding as described in Section IX.

[1] Agreement between the States Parties to the Convention for the establishment of a European Space Agency and the European Space Agency for the protection and exchange of classified information approved by ESA Council on 13 June 2002 and entered into force on 20 June 2003.

4. Identification of risks and mitigating plans and actions at ESA shall be managed as a process. This process shall be aimed at making a threat assessment, determining known security risks, defining security measures to reduce or mitigate risks in accordance with the present Regulations and at applying these measures in line with the concept of defence in depth. The effectiveness of such measures shall be continuously evaluated.

5. The security classification marking afforded to information shall be assigned in accordance with the degree of protection required to prevent the unauthorised disclosure of such information. The security classification system is the instrument for giving effect to these principles. This system of classification should provide the framework for the planning and organisation of countermeasures against unintentional release as well as from espionage, sabotage, terrorism and other threats.

6. The security measures addressed in the different Sections below:

   a) apply to all persons having access to Classified Information, Classified Information-carrying media, and all premises and critical installations containing such information;

   b) are designed to detect actions of persons who might endanger the security of Classified Information and important installations holding Classified Information, and to provide a mechanism for their exclusion or removal;

   c) prevent any unauthorised person from having access to Classified Information or to installations which contain it;

   d) ensure that Classified Information is disseminated solely on the basis of the need-to-know and to those having an appropriate and valid Personnel Security Clearance (PSC) for all information classified ESA CONFIDENTIAL and above;

   e) ensure the confidentiality, integrity, availability, authenticity and non-repudiation of all Classified Information, especially if handled in Communication and Information Systems (CIS).

7. The provisions of these Regulations shall be applicable at an equivalent level to ESA Contractors as defined in Annex 1 attached hereafter and to potential Contractors involved in the relevant Agency activities.

8. These Regulations may be revised by the ESA Council upon recommendation of the ESA Security Committee. Annexes appended to these Regulations may be updated by the ESA Security Committee.

SECTION II - ORGANISATION OF SECURITY

1. This Section sets out the provisions for implementing the responsibilities of the competent security authorities which are involved in the security measures related to the protection of Classified Information.

ESA MEMBER STATES

2. Each ESA Member State shall implement the ESA security standards as contained in these Regulations so as to ensure a common degree of protection for Classified Information; accordingly, it shall be responsible for:

   a) designating a National Security Authority (NSA)/Designated Security Authority (DSA) responsible for the security of ESA Classified Information;

   b) waiving of immunity of ESA Member States' representatives, in accordance with Article XIV.2 of Annex I of the ESA Convention and Article 7 of the Security Treaty when the concerned person is involved in a legal pursuit regarding the unauthorised disclosure of Classified Information.

3. In the framework of each ESA Member State administration, the corresponding NSA shall be responsible for:

   (a) the maintenance of the security of ESA Classified Information held by any national body or entity at home or abroad;

   (b) authorising the establishment of ESA TOP SECRET registries (this authority may be delegated to the ESA TOP SECRET Control Officer of a Central Registry);

   (c) the periodic inspection of the security arrangements for the protection of ESA Classified Information;

   (d) ensuring that all persons within a national body who in the conduct of their official duties require access or whose duties or function may afford access to ESA information classified ESA CONFIDENTIAL and above are appropriately security cleared before they are granted access to such information;

   (e) devising such contingency plans as are considered necessary to minimise the risk of a security breach and prevent ESA Classified Information from being compromised;

   (f) reporting actual or suspected breaches and compromises of ESA Classified Information to the ESA Security Office, and taking all appropriate measures, in accordance with national laws and regulations, when an incident occurs under their State's jurisdiction; and

   (g) coordinating security matters relating to protect ESA Classified Information with the competent security authorities as required.

ESA COUNCIL

4. The ESA Council shall be responsible for:

   (a) taking decisions on all issues related to security, in particular on an appropriate security policy, within ESA and in relation to the exchange of Classified Information with third States and International Organisations;

   (b) taking decisions whether to conclude a Security Agreement on the exchange of Classified Information with third States or International Organisations;

   (c) approving the Security Agreements and Memorandums of Understanding concerning the exchange of Classified Information with third States or International Organisations following a recommendation by the ESA Security Committee;

   (d) approving the measures resulting from the annual inspection reports for ESA and from the reports from third States and International Organisations;

   (e) approving the model template of a generic programme security instruction (PSI) applicable to any future ESA programme requiring protection of Classified Information; and

   (f) approving programme implementing rules applicable to ESA programmes requiring protection of Classified Information; and

   (g) waiving of the immunity, in accordance with Article IV.1.a) of Annex I to the ESA Convention and Article 7 of the Security Treaty, in all cases where it would impede the course of justice regarding an unauthorised disclosure of Classified Information, and in accordance with Article XXI.2 of the said Annex I in the case of the Director General.

ESA SECURITY COMMITTEE

5. The ESA Security Committee shall, in accordance with its terms of reference, advise the ESA Council and the Director General on all issues relating to the security of Classified Information. In this respect the ESA Security Committee shall:

   (a) prepare and submit recommendations to the ESA Council for it to consider and approve;

   (b) recommend the annual inspection programme for adoption by the ESA Council;

   (c) define and approve together with the concerned ESA Participating States the specific PSI, including its Classification Guide, for an ESA programme requiring protection of Classified Information;

(d) update, as necessary, the Annexes appended to the ESA Security Regulations;

(e) recommend to ESA Council the security legal instruments on the exchange of Classified Information with third States or International Organisations;

(f) recommend to ESA Council the measures to be taken following the results of the annual inspection reports for ESA and from third States and International Organisations;

(g) rely upon a dedicated panel (INFOSEC Panel) to provide, where necessary, expert advice to the ESA Security Committee on Information Assurance issues;

(h) approve the cryptographic products to be used by ESA.

ESA DIRECTOR GENERAL

6. The Director General shall in consultation with the ESA Security Committee as defined in paragraph 5 above:

(a) ensure the implementation of the ESA Security Regulations within ESA through the issuing of the necessary directives;

(b) address security issues referred to him by the ESA Security Office (ESO), by NSAs or DSAs;

(c) examine any proposals to change these ESA Security Regulations, in close liaison with the National Security Authority/Designated Security Authority (NSA/DSA) or any national competent security authority of the ESA Member States.

7. The Director General shall be responsible for:

(a) coordinating all matters of security relating to ESA activities;

(b) addressing to the competent security authorities of the ESA Member States requests for the NSA/DSA to provide security clearances for ESA Staff members and ESA experts in accordance with Section V;

(c) ordering from the ESA Security Office, supported as necessary by the competent security authorities, an investigation into any breach of security and/or compromise of Classified Information which, on prima facie evidence, has occurred at ESA, including in its IT Systems;

(d) requesting the appropriate competent security authorities to initiate investigations when a breach of security and/or the compromise of Classified Information appears to have occurred outside of ESA, and coordinating the enquiries when more than one competent security authority is involved;

(e) carrying out jointly and in agreement with the NSA/DSA concerned, periodic reviews of the security arrangements for the protection of ESA Classified Information in the ESA Member States;

(f) maintaining close liaison with all security authorities concerned in order to achieve overall coordination of security;

(g) keeping the ESA Security Regulations and procedures constantly under review and, as required, preparing appropriate recommendations. In this regard, he shall present to the ESA Council the annual inspection plan prepared by the ESA Security Office and recommended by the ESA Security Committee;

(h) accomplishing the necessary actions in order to establish a Central ESA TOP SECRET registry to be set up in ESA and to nominate the respective ESA authority;

(i) consulting the Agency Security Committee whenever the negotiation of draft cooperation agreements or implementing arrangements with third States or International Organisations addresses issues of security in the interest of the Agency;

(j) deciding on the release of Classified Information to a third State or an International Organisation following the successful conclusion of a Security Agreement or a Memorandum of Understanding; and

(k) waiving of an ESA staff's or expert's immunity, in accordance with the Article XXI.2 of Annex I of the ESA Convention and Article 7 of the Security Treaty, when the concerned person is involved in a legal pursuit regarding the unauthorised disclosure of Classified Information.

ESA SECURITY OFFICE

8. In order to fulfil the responsibilities mentioned in paragraphs 6 and 7 above, the Director General shall establish an ESA Security Office for the coordination, control and supervision of the implementation of the security measures. The ESA Security Office shall be in charge of the secretariat of the ESA Security Committee.

9. The Head of the ESA Security Office shall be responsible for:

(a) advising the Director General on security matters;

(b) coordination, supervision and control of the implementation of all security measures applicable to personnel, documents, physical infrastructure, Communications and Information Systems (CIS) in ESA, whether classified or unclassified, for both corporate general purpose and project-specific infrastructure;

(c) conduct of associated threat/risk assessments;

(d) security accreditation of the ESA security systems and personnel;

(e) authorising ESA staff to access Classified Information following confirmation from the NSA/DSA of an individuals' Personnel Security Clearance;

(f) audit of the correct implementation of the Security Regulations and relevant policies;

(g) production and maintenance of the Security Master Plan and the corresponding action plan;

(h) monitoring local security incident responses, liaising with national authorities, and initiating actions at ESA level, whenever necessary;

(i) conduct of a training and awareness programme on security matters;

(j) production and retention of security records and certificates, in line with relevant national requirements;

(k) acting as a custodian for all approved ESA Programme Security Instructions (PSIs), together with their classification guide, and ensuring the required updating of their annexes;

(l) preparation of the annual inspection programme for ESA and the inspection of third States and International Organisations to be submitted to the ESA Security Committee;

(m) carrying out the annual inspection programme for ESA and the inspection of third States and International Organisations as approved by the ESA Council;

(n) submitting the reports of the annual inspections for ESA and the inspection of third States and International Organisations to the ESA Security Committee;

(o) the accreditation of IT Systems and networks within ESA;

(p) acting as TEMPEST authority for ESA; and

(q) conducting upon request of the ESA Director General, investigations into any breach of security and/or compromise of Classified Information which, on prima facie evidence, has occurred in ESA, including its IT Systems.

10. The ESA Security Office shall have an INFOSEC Unit, responsible, inter alia, for issuing detailed guidance and defining the appropriate functions (INFOSEC, TEMPEST, CRYPTO Approval and CRYPTO Distribution Officers) on information assurance issues, based on the provisions of Section VI.

SECTION III - PHYSICAL SECURITY

1. This Section sets out the provisions for implementing the physical security measures for the protection of Classified Information.

2. Physical security is the application of physical and technical protective measures to prevent and/or delay unauthorised access to Classified Information. The competent security authorities, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented.

PHYSICAL SECURITY REQUIREMENTS AND MEASURES

3. All premises, areas, buildings, offices, rooms, Communication and Information Systems, in which Classified Information is stored and/or handled shall be protected by appropriate physical security measures.

4. Physical security measures shall be selected on the basis of a threat assessment made by the competent security authorities.

5. A risk management process shall be applied for the physical protection of Classified Information. The risk management process shall take account of all relevant factors, in particular:

   (a) the classification level of Classified Information;

   (b) the amount and form (e.g. paper copy or electronic copy) of the information held;

   (c) the surrounding environment and structure of the buildings or areas housing Classified Information;

   (d) the assessed threat from intelligence services which target ESA or ESA Member States and from sabotage, terrorist, subversive or other criminal activities. For ESA facilities this threat assessment shall be initiated by the ESA Security Office with the assistance of the relevant ESA service responsible for the implementation of security measures and in close liaison with the competent NSA of the host ESA Member State.

6. The physical security measures applied shall be designed to prevent or delay unauthorised access to Classified Information by:

   (a) denying surreptitious or forced entry by an intruder;

   (b) deterring, impeding and detecting unauthorised actions;

   (c) preventing those ESA Staff members or ESA experts, persons working for national bodies and/or for third States who do not have a need-to-know from having access to Classified Information

Complementary security safeguards shall be installed by the competent ESA service responsible for the implementation of security measures in close liaison with the Head of the Security Office where the planned activities of ESA require this.

7. The competent security authority, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented on the basis of an appropriate risk assessment. These can include one or more of the following:

   (a) a perimeter barrier: a physical barrier which defends the boundary of an area requiring protection;

   (b) Intrusion Detection Systems (IDS): an IDS may be used to enhance the level of security offered by a perimeter barrier, or in rooms and buildings in place of, or to assist, security staff;

   (c) access control: access control may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. Control may be exercised by electronic or electro-mechanical means, by security personnel and/or a receptionist, or by any other physical means;

   (d) security personnel: trained, supervised and, where necessary, appropriately security-cleared security personnel may be employed, inter alia, in order to deter individuals planning intrusion;

   (e) closed circuit television (CCTV): CCTV may be used by security personnel in order to verify incidents from unauthorised individuals or those without a need-to-know and IDS alarms on large sites or at perimeters;

   (f) security lighting: security lighting may be used to deter a potential intruder, as well as to provide the illumination necessary for effective surveillance directly by security personnel or indirectly through a CCTV system; and

   (g) any other appropriate physical measures to deter or detect unauthorised access or prevent or delay the compromise of Classified Information.

8. The competent security authority may authorise entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of Classified Information from premises or buildings.

9. When Classified Information is at risk from overlooking by unauthorised individuals or those without a need-to-know, appropriate measures shall be taken to counter the risk.

10. For new facilities, physical security requirements and their functional specifications shall be defined as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented to the maximum extent possible.

EQUIPMENT FOR THE PHYSICAL PROTECTION OF CLASSIFIED INFORMATION

11. When ESA is acquiring equipment (such as security containers, shredding machines, door locks, electronic access systems, IDS, CCTV, alarm systems) for the physical protection of Classified Information, the ESA competent security authority shall ensure that the equipment meets recognized European technical standards and minimum requirements.

12. ESA Member States whose facilities store and/or handle Classified Information may use nationally approved security equipment, as long as they offer a degree of protection at least equivalent to ESA requirements.

13. Security systems shall be inspected at regular intervals and equipment shall be maintained regularly. Maintenance work shall take account of the outcome of inspections to ensure that equipment continues to operate at optimum performance.

14. The effectiveness of individual security measures and of the overall security system shall be re-evaluated during each inspection.

PHYSICALLY PROTECTED AREAS

15. Two types of physically protected ESA areas shall be established for the physical protection of Classified Information: ESA Class II and ESA Class I.

16. For ESA facilities, the ESA Security Office shall establish if an area meets the requirements to be designated as an ESA Class II, an ESA Class I or an ESA Class I Technically Secured Area.

    (a) **ESA Class II**: this is an area to host the administration and management of the secured area and constitutes the area around and leading up to this secured area, providing the outer protective layer. In such area information up to and including ESA RESTRICTED can be handled and stored according to the provisions below:

        i) a visibly defined perimeter shall be established which allows all entry and exit controls of each individual and, where possible, each vehicle, by means of a pass or personal recognition system;

        ii) unescorted access shall be granted only to individuals who are duly authorised by the competent security authority;

        iii) all other individuals shall be escorted at all times or be subject to equivalent controls.

    (b) **ESA Class I**: this is an area where information ESA CONFIDENTIAL or above is handled and stored according to the provisions below:

(i) a visibly defined and protected perimeter shall be established through which all entries and exits are controlled by means of a pass or personal recognition system;

(ii) all visitors shall bear a specific authorisation to enter the area, shall be appropriately security cleared and shall be escorted at all times;

(iii) unescorted access shall be granted only to individuals who are appropriately security-cleared and specifically authorised to enter the area on the basis of their need-to-know.

(c) **ESA Class I Technically Secured Area:** this is an approved permanent or temporary area which is protected against eavesdropping as well as overlooking and where classified meetings can be held. The following additional requirements shall apply:

(i) such area shall be locked when not occupied and guarded when occupied;

(ii) all persons and material entering such area shall be controlled;

(iii) such area shall be regularly physically and/or technically inspected as required by the competent security authority;

(iv) such areas shall be free of communication lines, telephones or other communication devices and electrical or electronic equipment unless duly authorised and accredited;

(v) if such area has a temporary character, it will be physically and technically inspected prior to any use; the area shall be sealed and guarded in the time period between the physical and technical inspection and its actual use.

17. National competent security authorities shall establish that ESA Classified Information on the premises they are competent for will be handled and/or stored in areas deemed equivalent to that of paragraph 16 above.

GUARD PATROLS

18. Patrols of the Class II and Class I security areas (and, if any, the Class I Technically Secured Areas) shall take place outside normal working hours to protect Classified Information against security breaches and compromise. The frequency of the patrols will be determined by local circumstances and shall be conducted randomly.

PHYSICAL PROTECTION MEASURES FOR HANDLING AND STORING CLASSIFIED INFORMATION

19. Information classified ESA RESTRICTED shall be handled in such a way that it is protected from access by unauthorised individuals. It can be handled outside designated secure areas as long as unauthorised individuals do not have sight of the Classified Information. It shall be stored in suitable locked office furniture when not in use and provided the holder has undertaken to comply with additional protective measures laid down in security instructions issued by the competent security authority.

20. Information classified ESA CONFIDENTIAL or above shall be handled only in an ESA Class I security area or Technically Secured Area.

21. Information classified ESA CONFIDENTIAL or above shall be stored in a secured area in a security container or strong room with one or more of the following supplementary controls:

    (a) continuous protection or verification by cleared security staff or duty personnel;

    (b) an approved IDS in combination with response security personnel;

    (c) for security systems (alarm system, closed circuit television or other electrical devices) used to protect information classified ESA CONFIDENTIAL or above, an emergency electrical supply shall ensure the continuous operation of the systems if the main power supply is interrupted;

    (d) alarm or reliable warning for the surveillance personnel in case of any malfunctioning of or tampering with such systems;

    (e) two types of containers shall be used for the storage of Classified Information:

        (i) containers approved for the storage of information classified ESA TOP SECRET within a ESA Class I security area;

        (ii) containers approved for the storage of information classified ESA SECRET and ESA CONFIDENTIAL within an ESA Class I security area.

22. Strong rooms can be constructed within ESA Class I security areas. The walls, floors, ceilings, and lockable doors shall be approved by the competent security authority and afford protection equivalent to a security container approved for the storage of Classified Information of the same classification level.

23. Locks used with security containers and strong rooms in which information classified ESA CONFIDENTIAL or above is stored shall meet the recognized standards.

CONTROL OF KEYS, CODES AND COMBINATIONS USED FOR PROTECTING CLASSIFIED INFORMATION

24. The competent security authority shall define procedures for managing keys, codes and combinations for offices, rooms, strong rooms and security containers. The procedures shall be protected against unauthorised access.

25. Codes and combination settings shall be committed to memory by the smallest possible number of individuals needing to know them. Codes and combination settings for security containers and strong rooms storing Classified Information shall be modified:

    (a) on receipt of a new container;

    (b) whenever there is a change in personnel knowing the combination;

    (c) whenever a breach and/or compromise has occurred or is suspected;

    (d) when a lock has undergone maintenance or repair; and

    (e) at least every 12 months.

SECTION IV - MANAGEMENT OF CLASSIFIED INFORMATION

1. This Section sets out the provisions for implementing the management of Classified Information and it lays down the administrative measures for controlling Classified Information throughout its life-cycle in order to help deter, detect and recover from deliberate or accidental security breaches and/or compromise of such information. It details also the measures for the creation, distribution, transmission, storage, archiving, downgrading, declassification and destruction of Classified Information as well as the provisions for inspections and visit to ensure that the required minimum standards for protecting Classified Information are respected.

LEVELS OF CLASSIFICATION

2. ESA Classified Information shall be determined and marked in accordance with the following levels:

   (a) **ESA TOP SECRET**: this classification shall be applied only to information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of ESA and/or of one or more of its Member States.

   (b) **ESA SECRET**: this classification shall be applied only to information and material the unauthorised disclosure of which could seriously harm the essential interests of ESA and/or of one or more of its Member States.

   (c) **ESA CONFIDENTIAL**: this classification shall be applied to information and material the unauthorised disclosure of which could harm the essential interests of ESA and/or of one or more of its Member States.

   (d) **ESA RESTRICTED**: this classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of ESA and/or of one or more of its Member States.

3. Classified Information, as defined in Section I paragraph 2 above, and which is generated at national level, will bear an equivalent classification marking as outlined in Annex 2 attached hereafter.

CLASSIFICATION MANAGEMENT

4. Information shall be classified where it requires protection with regard to its confidentiality. The classification shall be clearly and correctly indicated and shall be maintained only as long as the information requires protection.

5. The originator of Classified Information shall be responsible for determining the security classification level, the initial dissemination of the information and any subsequent downgrading or declassification, in accordance with the relevant classification guidelines. The originator shall not over- or under-classify.

6. The number of persons authorised to originate ESA TOP SECRET documents shall be kept to a minimum and their names kept on a list drawn up by the ESA Director General and communicated to the ESA Member States.

7. The security classification shall be clearly and correctly indicated, regardless of whether the Classified Information is on paper, oral, electronic or in any other form.

8. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments or enclosures) may require different classifications and shall be marked accordingly, including when stored in electronic form.

9. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.

10. To the extent possible, documents containing parts with different classification levels shall be structured so that these parts may be easily identified and detached if necessary.

11. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator shall indicate clearly at which level it is classified when detached from its enclosures by means of an appropriate marking, e.g.:

ESA CONFIDENTIAL
Without attachment(s) ESA RESTRICTED

ADDITIONAL MARKINGS

12. In addition to one of the security classification markings set out in paragraph 2 above , Classified Information may bear additional markings, such as:

(a) an identifier to designate the originator;

(b) any caveats, code-words or acronyms specifying the field of activity to which the document relates, a particular distribution on a need-to-know basis or restrictions on use; specific provisions for the particular case of the caveat marking “CRYPTO” are defined in Section VI.

(c) releasability markings;

(d) where applicable, the date or specific event after which the Classified Information may be downgraded or declassified.

CREATION OF ESA CLASSIFIED INFORMATION

13. When creating an ESA classified document:

    (a) each page shall be marked clearly at the top and the bottom with the classification level;

    (b) each page shall be numbered;

    (c) the document shall bear a reference number and a subject, which is not itself Classified Information, unless it is marked as such;

    (d) the document shall be dated;

    (e) documents classified ESA CONFIDENTIAL or above, and all documents carrying the caveat marking CRYPTO, shall bear a copy number on every page if they are to be distributed in several copies.

14. When ESA Classified Information cannot be marked as described in paragraph 13 above, other appropriate measures shall be taken.

15. At the time of its creation, the originator shall indicate, where possible, whether ESA Classified Information can be downgraded or declassified on a given date or following a specific event.

16. ESA Registries (where Classified Information is registered, handled and stored) and its subordinate registries shall regularly review ESA Classified Information to ascertain whether the classification level still applies. Such a review shall not be necessary where the originator has indicated from the outset that the information will automatically be downgraded or declassified and the information has been marked accordingly.

REGISTRATION OF CLASSIFIED INFORMATION

17. Within ESA and ESA Member States' national administrations in which Classified Information is handled, registries shall ensure that information classified ESA CONFIDENTIAL or above is handled in accordance with these Regulations. ESA Registries shall be established in ESA Class I areas as defined in Section III.

18. For the purpose of these Regulations, registration for security purposes (hereinafter referred to as "registration") means the application of procedures which record the life-cycle of material, including its distribution, transmission, storage and destruction.

19. All information classified ESA CONFIDENTIAL or above shall be registered in appropriate registries when it arrives or leaves.

20. The ESA Central Registry of the ESA Security Office shall keep a record of all information classified ESA CONFIDENTIAL or above released to or received from an ESA Member State, a third State or International Organisation.

21. In the case of a Communication and Information System, registration procedures may be performed by processes within the Communication and Information System itself.

ESA TOP SECRET REGISTRIES

22. A registry authority shall be designated at ESA and at each ESA Member State's national administration to act as the central receiving and dispatching authority for information classified ESA TOP SECRET. Where necessary, subordinate registries may be designated to handle such information for registration purposes.

23. The ESA TOP SECRET registry authority is responsible for:

    (a) the transmission of ESA TOP SECRET information in accordance with these Regulations;

    (b) maintaining a list of all its dependent ESA TOP SECRET subordinate registries together with names and signatures of the appointed registrars and their authorised deputies;

    (c) holding receipts from registries for all ESA TOP SECRET information distributed in the Agency;

    (d) the physical safeguarding of all ESA TOP SECRET documents held within the registry in accordance with these Regulations.

24. The appointed registrars of an ESA TOP SECRET subordinate registry shall be responsible for:

    (a) the secure transmission of ESA TOP SECRET information in accordance with these Regulations;

    (b) maintaining an up-to-date list of all persons authorised to have access to the ESA TOP SECRET information under the registrar's control;

    (c) maintaining an up-to-date record of all ESA TOP SECRET documents held or circulating under his control or which have been passed to other ESA TOP SECRET subordinate registries and holding all corresponding receipts;

    (d) maintaining an up-to-date list of ESA TOP SECRET subordinate registries with which he is authorised to exchange ESA TOP SECRET information, together with the names and signatures of their registrars and authorised deputies; and

(e) the physical safeguarding of all ESA TOP SECRET information held within the subordinate registry in accordance with these Regulations.

25. Every twelve months, each ESA TOP SECRET registry and subordinate registry shall carry out an itemised inventory of all ESA TOP SECRET information for which it is accountable. Information is deemed to have been accounted for if the registry physically musters the information, or holds a receipt from the ESA TOP SECRET registry to which the document has been transferred, a destruction certificate for the information or an instruction to downgrade or declassify the information.

26. ESA TOP SECRET subordinate registries shall forward the findings of their annual inventory to the central ESA TOP SECRET registry on a date specified by the latter.

27. Every year, by 31 March at the latest, all ESA TOP SECRET registry authorities shall forward to the ESA Director General the findings of the annual inventories conducted by the ESA Security Office, provided any ESA TOP SECRET information has been handled or stored.

28. Subordinate registries may not transmit ESA TOP SECRET documents directly to other subordinate registries of the same ESA TOP SECRET central registry or externally without the express written approval of the latter.

COPYING AND TRANSLATING CLASSIFIED DOCUMENTS

29. Copying of Classified documents should be kept to the minimum essential for the efficient conduct of business. Spare copies should be reviewed regularly for destruction.

30. ESA TOP SECRET documents shall not be copied or translated without the prior written consent of the originator. The destination of any copies made must be recorded.

31. Where the originator of documents classified ESA SECRET or below has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder. The security measures applicable to the original document shall apply to copies and translations hereof.

TRANSMISSION OR CARRIAGE OF CLASSIFIED INFORMATION

32. Transmission or carriage of Classified Information between services and premises outside physically protected areas shall:

(a) as a general rule, transmission shall be done by electronic means, protected by cryptographic products approved in accordance with Section VI;

(b) when the means referred to in point (a) are not used, be made either:

(i) on electronic media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products approved in accordance with Section VI; or

(ii) in all other cases, as prescribed by the competent security authority in accordance with the relevant protective measures laid down in the provisions of paragraphs 33, 35, 36, 37 and 38 below.

33. Transmission or carriage of documents classified ESA CONFIDENTIAL or above between ESA Member States or to third States or International Organisations shall be done in appropriate, opaque double envelopes. The inner envelope shall be marked with the appropriate ESA security classification as well as the recipients name, job title and address. Both the outer and inner envelope/package should include a return address on the back in the event that delivery cannot be made. The outer envelope shall carry sufficient detail to ensure correct delivery.

34. The competent security authorities in ESA and in the ESA Member States shall issue instructions on the transmission of ESA Classified Information in accordance with these Regulations.

TRANSMISSION OR CARRIAGE OF CLASSIFIED INFORMATION WITHIN A BUILDING OR SELF-CONTAINED GROUP OF BUILDINGS

35. Transmission or carriage of Classified Information within a building or a self-contained group of buildings shall be covered in order to prevent observation of its contents.

36. Transmission or carriage of information classified ESA TOP SECRET within a building or self-contained group of buildings, shall be done by means of a sealed envelope bearing only the addressee's name.

TRANSMISSION OR CARRIAGE OF CLASSIFIED INFORMATION WITHIN AND BETWEEN ESA MEMBER STATES

37. Transmission or carriage of information classified ESA TOP SECRET between buildings or premises within and between ESA Member States shall be done by official courier or by persons authorised to have access to ESA TOP SECRET information. Whenever an official courier is used for the transmission of ESA TOP SECRET information, the packaging and receipting provisions contained in these Regulations shall be complied with. Delivery services shall be so staffed as to ensure that packages containing ESA TOP SECRET information remain under the direct supervision of a responsible official at all times.

38. Transmission or carriage of information classified ESA CONFIDENTIAL and ESA SECRET within or between ESA Member States' territories shall be done by one of the following means:

(a) military, government or diplomatic courier, as appropriate;

(b) hand carriage, provided that:

i) the Classified Information does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Section III;

ii) the Classified Information is not opened “en route” or read in public places;

iii) individuals are briefed on their security responsibilities;

iv) individuals are appropriately cleared and provided with a courier certificate where necessary;

39. Transmission or carriage of information classified ESA CONFIDENTIAL may be done by postal services or commercial courier services, provided that:

(a) they are approved by the relevant NSA in accordance with national laws and regulations;

(b) they apply appropriate protective measures in accordance with minimum requirements to be laid down accordingly in specific internal security instructions; and

(c) the transmission is done from the authorised sender to the addressee in person or a person appropriately delegated to receive the consignment.

40. Transmission or carriage of material classified ESA CONFIDENTIAL and ESA SECRET (e.g. equipment or machinery) which cannot be transmitted or carried by the means referred to in paragraph 38 above shall be transported as freight by commercial carrier companies in accordance with the provisions of Section VII.

41. Transmission or carriage of information classified ESA RESTRICTED shall be done in accordance with national rules and regulations and by:

a) normal or registered mail, as appropriate;

b) commercial courier services;

c) hand-carriage without formal courier order, provided that during travel, the items remain under permanent personal custody and may not be left unattended in hotel rooms or vehicles and may not be read in public; or electronic means in accordance with the provisions of Section VI.

TRANSMISSION OR CARRIAGE OF CLASSIFIED INFORMATION FROM WITHIN ESA MEMBER STATES TO THE TERRITORY OF A THIRD STATE OR INTERNATIONAL ORGANISATION

42. Transmission or carriage of Classified Information from within ESA Member States to the territory of a third State or to an International Organisation shall be

covered in order to prevent observation of its contents, in accordance with the following provisions.

43. Transmission or carriage of information classified ESA TOP SECRET from within ESA Member States to the territory of a third State or to an International Organisation shall be made by military, government or diplomatic courier, as appropriate provided it complies with the relevant provisions of a Security Agreement in accordance with Section IX and with the relevant ESA Council decision;

44. Transmission or carriage of information classified ESA CONFIDENTIAL and ESA SECRET may be done by ESA to a third State or International Organisation, provided it complies with the relevant provisions of a Security Agreement in accordance with Section IX , and with the relevant ESA Council decision; in any case, such provisions shall not be less stringent than the provisions laid down in paragraph 38 of this Section.

45. Transmission or carriage of information classified ESA RESTRICTED may be done by postal services or commercial courier services.

DOWNGRADING AND DECLASSIFICATION OF CLASSIFIED INFORMATION

46. Classified Information should be downgraded when protection is no longer needed at the original level, or declassified when protection is no longer necessary.

47. The originator of the Classified Information is solely responsible for taking the decision to downgrade or declassify. If the Classified Information contains sensitive information provided from other sources (e.g. other Member States) then the originator should consult the interested parties before taking a decision to downgrade or declassify.

48. If the originator of Classified Information cannot be identified then ESA will assume responsibility and the information can be downgraded and declassified in accordance with internal ESA procedures.

DESTRUCTION OF CLASSIFIED INFORMATION

49. Classified documents which are no longer required may be destroyed without prejudice to the relevant rules and regulations on archiving.

50. Classified documents, shall be destroyed in accordance with national rules and regulations and, in the case of ESA, according to instructions from the ESA Security Office, so as to prevent reconstruction in whole or in part.

51. Classified documents subject to registration shall be destroyed by the responsible registry on instruction from the holder or from a competent security authority. The logbooks and other registration information shall be updated accordingly.

52. Documents classified ESA SECRET and above may only be destroyed in the presence of a witness who shall be cleared at least for the classification level of the document to be destroyed. Documents classified ESA TOP SECRET may only be destroyed by the central ESA TOP SECRET registry.

53. All Classified Information provided by third States and International Organisations that is required to be destroyed shall be done so in a manner consistent with the relevant Security Agreement or Memorandum of Understanding with that third State or International Organisation. A destruction certificate shall be filed in the registry for information classified ESA CONFIDENTIAL and above. Where required by the provisions of the Security Agreement or Memorandum of Understanding the third State or International Organisation shall be informed by the ESA Security Office of such destruction.

54. The registrar and the witness, where the presence of the latter is required, shall sign a destruction certificate listing each destroyed document classified ESA SECRET and above, which shall be filed in the registry. The registry shall keep destruction certificates of ESA TOP SECRET documents for a period of at least ten years and of documents classified ESA SECRET for a period of at least five years.

55. The destruction of computer storage media used for Classified Information shall be in accordance with the prescriptions of Section VI.

DESTRUCTION OF CLASSIFIED INFORMATION IN CASE OF EMERGENCY

56. The ESA Security Office and the ESA Member States shall prepare plans based on local conditions for the safeguarding of Classified Information in a crisis including, if necessary, emergency destruction and evacuation plans; they shall promulgate instructions deemed necessary to prevent Classified Information from falling into unauthorised hands.

57. The arrangements for the safeguarding and/or destruction of information classified ESA CONFIDENTIAL or ESA SECRET in a crisis shall under no circumstances adversely affect the safeguarding or destruction of information classified ESA TOP SECRET, including the enciphering equipment, whose treatment shall take priority over other tasks. The measures to be adopted for the safeguarding and destruction of enciphering equipment in an emergency shall be in accordance with Section VI.

ARCHIVE STORAGE OF CLASSIFIED INFORMATION WITHIN ESA

58. ESA records and archives, whatever their level of classification, are an integral part of the Agency's property, resources and assets and must be handled accordingly. The ESA Documents and Records Management Policy related to archiving Classified Information shall be consistent with the applicable security provisions laid down in these Regulations.

59. In cooperation and consultation with the ESA Records Manager, the ESA central registrar may store and archive Classified Information up to and including ESA SECRET level on magnetic or optical media, provided:

(a) the process is undertaken by appropriately cleared personnel;

(b) the storage medium is afforded the same security protection as the original information;

(c) the storing of ESA CONFIDENTIAL and ESA SECRET information is clearly indicated in the record used for the annual inventory; and

(d) in the case of destruction the above provisions apply.

INSPECTIONS AND ASSESSMENT VISITS

60. Inspections and assessment visits shall be carried out, inter alia, to:

(a) ensure that the required minimum standards for protecting Classified Information laid down in these Regulations are respected;

(b) emphasise the importance of security and effective risk management within the entities inspected;

(c) recommend countermeasures to mitigate the specific impact of loss of confidentiality, integrity or availability of Classified Information;

(d) reinforce competent security authorities' ongoing security education and awareness programmes.

For the purpose of the following paragraphs, the term "inspections" applies to both inspections and assessment visits.

61. Before the end of each calendar year, the ESA Security Committee shall recommend the inspection and assessment visits plan for adoption by the ESA Council. The actual dates for each inspection shall be determined in agreement with the competent security authorities for the relevant facilities, at ESA, in ESA Member States, third States or International Organisations concerned.

CONDUCT OF INSPECTIONS AND ASSESSMENT VISITS

62. Inspections can be conducted in two phases. Prior to the inspection itself a preparatory meeting may be organised, if necessary, with the entity concerned. After this preparatory meeting the inspection team shall establish, in agreement with the said entity, a detailed inspection programme covering all areas of security.

63. For ESA facilities the inspection team shall have access to any location where Classified Information is handled, in particular registries and Communication and Information System points of presence.

64. Inspections of ESA facilities, sites or stations shall be conducted by the ESA Security Office with the assistance of experts of the NSA/DSA on whose territory the facilities are located.

65. Inspections in ESA Member States' national administrations shall be conducted by the ESA Security Office, in mutual agreement and in full cooperation with the NSA/DSA in question.

66. Inspections in third States' national administrations and in International Organisations shall be conducted under the responsibility of a joint ESA/ESA Member States inspection team in full cooperation with the officials of the third State or International Organisation being inspected.

INSPECTION REPORTS

67. At the end of the inspection, the main conclusions and recommendations shall be presented to the inspected entity. Thereafter, a report on the inspection shall be drawn up under the responsibility of the ESA Security Office. Where corrective actions and recommendations have been proposed, sufficient details shall be included in the report to support the conclusions reached.

68. The draft inspection report shall be forwarded to the entity or body concerned to verify that it is factually correct and that it contains no information classified higher than ESA RESTRICTED. Any corrective action shall be verified during a follow-up visit and reported to the ESA Security Committee.

69. Final inspection reports may be distributed to all members of the ESA Security Committee. For inspections conducted in Member States' national administrations the NSA in question may request that general distribution to the ESA Security Committee is withheld. Should a NSA withhold distribution, it shall submit, in writing to the ESA Security office, the reasons for such withholding.

70. A regular report shall be prepared by the ESA Security Office to highlight the lessons learned from the inspections conducted over a specified period. This regular report shall be submitted to the ESA Security Committee.

71. For assessment visits of third States and International Organisations, the report shall be distributed to the ESA Security Committee. If appropriate, the report shall be classified at least ESA RESTRICTED. Any corrective action shall be verified during a follow-up visit and reported to the Security Committee.

INSPECTIONS CHECKLIST

72. The ESA Security Office shall draw up and update a security inspection checklist of items to be verified in the course of an inspection. The inspection checklist is to be seen as a guideline for the inspectors and it is not limitative.

73. The information to complete the checklist shall be obtained in particular during the inspection from the security management of the entity being inspected. Once

completed with detailed responses, the checklist may be classified in agreement with the inspected entity. It shall not form part of the inspection report.

SECTION V - PERSONNEL SECURITY

1. This Section sets out provisions for the measures regarding the security of personnel and lays down in particular the criteria for determining whether an individual may be authorised to have access to, and generate Classified Information, and the investigative and administrative procedures to be followed by the competent security authorities of the Member States to grant a Personnel Security Clearance.

2. Throughout this Section, the term "Personnel Security Clearance" (PSC) shall refer to the clearance granted by a competent security authority of an ESA Member State.

3. Any individual that by reason of his duties and for the requirements of his task needs to have knowledge of ("need-to-know"), or to use information classified ESA CONFIDENTIAL or above, shall have a PSC and be duly authorised by ESA.

ACCESS TO CLASSIFIED INFORMATION

4. An individual shall only be authorised to access information classified ESA CONFIDENTIAL or above after:

   (a) his "need-to-know" has been determined;

   (b) he has been granted a PSC by the competent security authority to the relevant level or is otherwise duly authorised by virtue of his functions to access Classified Information in accordance with national laws and regulations;

   (c) he has been briefed on the security rules and procedures for protecting Classified Information and has acknowledged his responsibilities with regard to protecting such information.

5. Any individual that by reason of his duties and for the requirements of his task needs to have knowledge of ("need-to-know"), or to use information classified ESA RESTRICTED, is not required to have a PSC. Such individuals shall be briefed on the security rules and procedures for protecting Classified Information and on their responsibilities regarding the protection of such information.

6. ESA Staff members, ESA experts and employees of ESA contractors employed in ESA facilities meeting the requirements and criteria listed in paragraph 4 above shall in addition need an Authorisation to Access Classified Information (AACI) to be granted by the ESA Security Office.

7. A list of ESA posts requiring access to information classified ESA CONFIDENTIAL or above shall be drawn up and kept up to date by the ESA Security Office. The names of all persons ceasing to be employed on duties requiring access to information ESA CONFIDENTIAL or above, shall be removed from this list. A declaration stating that they will neither use nor pass on

Classified Information they have knowledge about shall be signed by the persons concerned.

PERSONNEL SECURITY CLEARANCE (PSC) REQUESTS

8. The ESA Security Office is responsible for drawing up the PSC requests for ESA Staff members, ESA experts and employees of ESA contractors employed in an ESA facilities who, by reason of their duties and for the requirements of their task, need to have knowledge of, to use, or generate Classified Information. The request shall specify the type, amount and level of Classified Information to be made available to the person concerned. The request shall also provide the justifications for the requested level of the Personnel Security Clearance.

9. The request for a PSC shall be sent to the NSA/DSA of the ESA Member State of which the person concerned is a national. Where the person concerned is a national of a third State, the request for a PSC shall be addressed to the NSA/DSA of the ESA Member State of the ESA facility in which he is employed, depending on and subject to this ESA Member States' national laws and regulations.

10. Should the individual concerned reside in the territory of another ESA Member State or of a third State, the competent national security authorities shall seek assistance from the competent security authority of the State of residence in accordance with the host nations' laws and regulations.

11. After having received a request from the ESA Security Office, the NSAs or other national competent security authorities shall ensure that security investigations are carried out. Standards of investigation shall be conducted in accordance with criteria described in paragraphs 13, 14 and 15 of this Section. NSAs/DSAs of ESA Member States shall assist one another in carrying out security investigations in accordance with their national laws and regulations.

INVESTIGATIVE REQUIREMENTS FOR A PERSONNEL SECURITY CLEARANCE – ESA SECRET AND ESA CONFIDENTAL

12. The PSC for access to information classified ESA CONFIDENTIAL and ESA SECRET shall be based on a security investigation executed by the relevant NSA/DSA and shall cover at least the last five years, or from age 18 to present, whichever is the shorter. The relevant NSA/DSA shall make an overall assessment based on the findings of such a security investigation. No single adverse finding shall necessarily constitute a reason to deny a PSC. The PSC, when granted, shall be valid for a period not exceeding ten years with effect from the date of notification of the outcome of the last security investigation on which they were based.

13. To the extent possible under national laws and regulations the security investigation for a PSC shall include the following :

    (a) a completed national personnel security questionnaire or national equivalent for the level of Classified Information to which the individual

may require access; once completed, this questionnaire shall be forwarded to the appropriate competent security authority by the ESA Security Office;

(b) an identity check/citizenship/nationality status – the individual's date and place of birth shall be verified and his identity checked. Citizenship status and/or nationality, past and present, of the individual shall be established; and

(c) a national and local records check – a check shall be made of national security and central criminal records, where the latter exist, and/or other comparable governmental and police records. The records of law enforcement agencies with legal jurisdiction where the individual has resided or been employed shall be checked.

In addition to the above, the criteria listed below shall be included, to the extent possible in accordance with the respective national laws and regulations:

(d) a verification whether the individual has committed or attempted to commit, conspired with or aided and abetted another to commit any act of espionage, terrorism, sabotage, treason or sedition;

(e) a check if the person is, or has been, an associate of spies, terrorists, saboteurs or of individuals reasonably suspected of being such or an associate of representatives of organisations of foreign states, including foreign intelligence services, which may threaten the security of ESA and/or its Member States unless these associations were authorised in the course of official duty;

(f) a verification whether the individual is, or has been, a member of any organisation which by violent, subversive or other unlawful means seeks, inter alia, to overthrow the government of an ESA Member State, to change the constitutional order of an ESA Member State or to change the form or the policies of its government;

(g) a check if the person is, or has been, a supporter of any organisation described in point (f), or who is, or who has been closely associated with members of such organisations;

(h) a verification whether the individual has deliberately withheld, misrepresented or falsified information of significance, particularly of a security nature, or has deliberately lied in completing a personnel security questionnaire or during the course of a security interview;

(i) a check if the person has been convicted of a criminal offence or offences;

(j) a verification whether the individual has a history of alcohol dependence, use of illegal drugs and/or misuse of legal drugs;

(k) a check if the person is or has been involved in conduct which may give rise to the risk of vulnerability to blackmail or pressure;

(l) a verification whether the individual by act or through speech, has demonstrated dishonesty, disloyalty, unreliability or untrustworthiness;

(m) a check if the person has seriously or repeatedly infringed security regulations; or has attempted, or succeeded in, unauthorised activity in respect of Communication and Information Systems;

(n) a verification whether the individual may be liable to pressure (e.g. through holding one or more third State nationalities or through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations, or individuals whose aims may threaten the security interests of ESA and/or its Member States);

(o) a check on the individual's financial and medical background, if considered relevant or essential for the ESA Member States' PSC procedures and in accordance with the national laws and regulations;

(p) a verification concerning the person's spouse's, cohabitant's or close family member's character, conduct and circumstances, if considered relevant during the security investigation and necessary for the ESA Member States' PSC procedures in accordance with the national laws and regulations.

INVESTIGATIVE REQUIREMENTS FOR A PERSONNEL SECURITY CLEARANCE – ESA TOP SECRET

14. The PSC for access to information classified ESA TOP SECRET shall be based on a security investigation covering at least ten years, or from age 18 to present, whichever is shorter. If interviews are conducted as stated in point (e) below, investigations shall cover at least the last seven years, or from age 18 to the present, whichever is shorter. The PSC, when granted, shall be valid for a period not exceeding five years with effect from the date of notification of the outcome of the last security investigation on which they were based. In addition to the criteria indicated in paragraph 13 above, the following elements shall be investigated, to the extent possible under national laws and where required by national laws and regulations, before granting an ESA TOP SECRET PSC; they may also be investigated before granting an ESA CONFIDENTIAL or ESA SECRET PSC, where required by national laws and regulations:

(a) financial status – information shall be sought on the individual's finances in order to assess any vulnerability to foreign or domestic pressure due to serious financial difficulties, or to discover any unexplained affluence;

(b) education – information shall be sought to verify the individual's educational background at schools, universities and other education establishments attended since his 18th birthday, or during a period judged appropriate by the investigating authority;

(c) employment – information covering present and former employment shall be sought, reference being made to sources such as employment records, performance or efficiency reports and to employers or supervisors;

(d) military service – where applicable, the service of the individual in the armed forces and type of discharge shall be verified; and

(e) interviews – where provided for and admissible under national law, an interview or interviews shall be conducted with the individual. Interviews shall also be conducted with other individuals who are in a position to give an unbiased assessment of the individual's background, activities, loyalty, trustworthiness and reliability. When it is national practice to ask the subject of the investigation for referrals, referees shall be interviewed unless there are good reasons for not doing so.

15. Where necessary and in accordance with national laws and regulations, additional investigations may be conducted to develop all relevant information available on an individual and to substantiate or disprove adverse information.

GRANTING OF A PERSONNEL SECURITY CLEARANCE

16. Following the completion of the security investigation, the relevant NSA/DSA shall notify the ESA Security Office of the outcome of such an investigation.

17. Where relevant information concerning an individual who has applied for a PSC becomes known to ESA, the ESA Security Office shall notify the relevant NSA/DSA.

RENEWAL OF A PERSONNEL SECURITY CLEARANCE

18. After a PSC was granted and provided that the individual has had uninterrupted service with a national administration or with ESA and has a continuing need for access to Classified Information, the PSC shall be reviewed and renewed based on security investigations which covers the period elapsed since the previous investigation.

19. For the renewal of PSCs, the elements outlined in paragraphs 13 and 14 above shall be investigated, in accordance with national laws and regulations.

20. Requests for renewal shall be made in a timely manner taking account of the time required for security investigations. Nevertheless, where the relevant national competent security authority has received the request for renewal and the corresponding personnel security questionnaire before a PSC expires, and the necessary security investigation has not been completed, the national competent security authority may, where admissible under national laws and regulations, extend the validity of the existing PSC for a period of up to 12 months. If, at the end of this 12-month period, the security investigation has still not been completed, the individual shall not be allowed to access information classified CONFIDENTIAL or above until the renewed PSC is granted.

GRANTING AND/OR RENEWAL OF THE AUTHORISATION TO ACCESS CLASSIFIED INFORMATION (AACI)

21. When a PSC has been granted or renewed, the ESA Security Office may grant an ESA Authorisation to Access Classified Information (AACI) to the individual concerned and authorise access to Classified Information up to the relevant level until a specified date. The date of the AACI will not exceed that of the individuals' PSC.

22. All ESA employees who were granted a PSC shall receive all necessary instructions concerning the protection of Classified Information and the means of ensuring such protection. When granted an AACI such persons shall sign an "Acceptance of Responsibility Declaration", acknowledging the receipt of the instructions, their individual responsibility, their undertaking to obey the relevant rules and regulations and in particular of having been informed on the consequences as described in paragraph 12 of Section X. The "Acceptance of Responsibility" shall be kept on file by the ESA Security Office.

DENIAL OR WITHDRAWAL OF A PERSONNEL SECURITY CLEARANCE

23. Where information becomes known to the NSA/DSA concerning a security risk posed by an individual, the NSA/DSA may withdraw the PSC and shall notify ESA thereof. The denial or the withdrawal of a PSC shall be subject to the relevant laws and regulations in force in the ESA Member State concerned, including those concerning appeals.

DENIAL OR WITHDRAWAL OF THE AUTHORISATION TO ACCESS CLASSIFIED INFORMATION

24. When no PSC can be granted, no AACI is given and the ESA Security Office shall notify the individual concerned, who may ask to be heard by the ESO and/or by the ESA Director General. The ESA Security Office may in these cases ask the relevant NSA/DSA for any further clarification it can provide according to its national laws and regulations.

25. The denial or the withdrawal of the AACI by ESA Security Office shall be subject to appeals in accordance with the ESA Staff Regulations, Rules and Instructions or the contractual stipulations, whichever are relevant.

RECORDS OF PERSONNEL SECURITY CLEARANCES

26. Records of PSCs granted for access shall be maintained respectively by each ESA Member State and by the ESA Security Office. These records shall contain as a minimum the level of ESA Classified Information to which the individual may be granted access, the date the PSC was granted and its period of validity.

27. Records are only required for the level of ESA CONFIDENTIAL and above, as no PSC is required for access to information classified ESA RESTRICTED.

EXEMPTIONS FROM THE PERSONNEL SECURITY CLEARANCE REQUIREMENT

28. Based on a written statement of the competent national security authority, the Head of the ESA Security Office may grant access to Classified Information to individuals of ESA Member States who are duly authorised to access Classified Information by virtue of their functions in accordance with the laws and regulations of the country concerned. Such individuals shall be briefed on their obligations in respect of protecting Classified Information by their competent national security authority.

29. Exceptionally, and in accordance with applicable national rules and regulations, the Head of the ESA Security Office may grant a temporary authorisation to an ESA Staff member to access information classified up to and including ESA SECRET only for a specific function for reasons of urgency, where duly justified and pending the completion of a full security investigation.

    To this extent, the ESA Security Office shall consult with the NSA/DSA of the Member State of whom the individual is a national.

    ESA is to warrant for the incumbent in this period, based on the outcome of preliminary checks to verify that no adverse information is known.

    Such temporary authorisation shall be valid for a period not exceeding six months and shall not permit access to information ESA TOP SECRET.

    All individuals who have been granted a temporary authorisation shall acknowledge in writing that they have understood their obligations in respect of protecting the Classified Information they are granted access to and the consequences should this information be compromised.

SECTION VI - CLASSIFIED INFORMATION HANDLED IN COMMUNICATION AND INFORMATION SYSTEMS

1. This Section sets out the provisions for implementing the security measures for the handling of the Classified Information in Communication and Information Systems (CIS). All Systems require security measures to protect the integrity and availability of those Systems and of the information they contain and may require additional measures to protect confidentiality and assure authenticity and non–repudiation as described in this Section.

2. For the security and correct function of operations in Information Technology and Communications Systems the following basic principles shall apply:

   (a) authenticity: the guarantee that information is genuine and from bona fide sources;

   (b) availability: the property of being accessible and usable upon request by an authorised entity;

   (c) confidentiality: the property that information is not disclosed to unauthorised individuals, entities or processes;

   (d) integrity: the property of safeguarding the accuracy and completeness of information and assets;

   (e) non-repudiation: the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.

3. The System-specific security measures shall be determined by the designated Security Accreditation Authority (SAA) on the basis of a risk management process, subject to continuous improvement according to the plan-do-check-act principle, according to the ISO 27000 family of standards. CIS shall handle ESA Classified Information in accordance with the concept of Information Assurance.

THREATS AND VULNERABILITIES OF IT SYSTEMS

4. A threat can be defined as a potential for the accidental or deliberate breach and/or compromise of information, involving loss of one or more of the properties of information assurance.

5. A vulnerability can be defined as a weakness or lack of controls that would facilitate or allow a threat actuation against a specific asset, i.e. anything that is of value to the organisation, especially the CIS that support the organisation's mission. A vulnerability may be an omission or it may relate to a deficiency in a control's strength, completeness or consistency; it may be technical, procedural or operational in nature.

6. When a threat is applied to a vulnerability, a risk is present that damage may occur to an asset, which is to be avoided or mitigated by appropriate security measures. The ESA Director General shall identify a risk owner within the organisation, who will take care of enacting and funding these measures.

7. In the case of security breach or compromise, immediate action shall be taken by the responsible NSA/DSA and/or the ESA Security Office, which shall be responsible for recording and analysing the data and take appropriate actions, pursuant to the provisions of Section X.

SECURITY MEASURES FOR IT SYSTEMS

8. The main purpose of the security measures stated in this Section is to provide protection against unauthorised disclosure of information (the loss of confidentiality) and against the loss of integrity or availability of information. To achieve adequate security protection of a System handling Classified Information, the appropriate standards of conventional security shall be applied according to the level of Classified Information to be protected, along with appropriate special security procedures and techniques uniquely designed for each System.

9. A balanced set of security measures shall be identified and implemented to create a secure environment in which a System operates. The fields of application of those measures concern physical elements, personnel, non-technical procedures, computer and communications operating procedures.

10. Computer security measures (hardware and software) shall be required to implement the need-to-know principle, and to prevent or detect the unauthorised disclosure of information. The extent to which computer security measures are to be relied upon shall be determined during the process of establishing the security requirements, on the basis of a risk management exercise. The process of accreditation shall determine that an adequate level of assurance is present to support this reliance on computer security measures.

11. To mitigate risk to an IT System, a range of technical and non-technical security measures, organised as multiple layers of defence (defence in depth), shall be implemented. These layers shall include:

    (a) deterrence: security measures aimed at dissuading any adversary planning to attack the System;

    (b) prevention: security measures aimed at impeding or blocking an attack on the System;

    (c) detection: security measures aimed at discovering the occurrence of an attack on the System;

    (d) resilience: security measures aimed at limiting impact of an attack to a minimum set of information or assets and preventing further damage, and

(e) recovery: security measures aimed at regaining a secure situation for the System if it is compromised.

The degree of stringency of such security measures shall be determined following a risk assessment.

SECURITY OF INFORMATION CLASSIFIED ESA RESTRICTED IN AN IT SYSTEM

12. Security measures must be in place when processing or transmitting information classified ESA RESTRICTED on IT Systems, in accordance with the provisions of paragraph 62 below, so as to ensure its traceability and controlled distribution.

13. Information classified ESA RESTRICTED, when not in use, shall be encrypted with a tool approved by the SAA on the basis of the provisions of paragraph 47 below.

14. Computers where information classified ESA RESTRICTED is in use in clear shall not be connected to an unclassified network (e.g. the Internet or the cellular network) except where the provisions of paragraph 44 below apply.

SECURITY MODES OF OPERATION

15. All Systems handling information classified ESA CONFIDENTIAL and above shall be accredited to operate in one, or where warranted by requirements during different time periods, more than one, of the following security modes of operation, as further defined in Annex 1 attached hereafter, or in their national equivalent standards for information classified ESA CONFIDENTIAL and above:

(a) “Dedicated Security”;

(b) “System High Security”;

(c) “Multi-Level Security”.

ADDITIONAL MARKINGS

16. Additional markings such as CRYPTO or any other ESA recognised special handling designator shall apply where there is a need for limited distribution or special handling in addition to that designated by the security classification.

SECURITY ACCREDITATION AUTHORITY (SAA)

17. The SAA shall be either:

(a) an NSA/DSA or other competent security authority, when the System handling Classified Information is deployed under its national responsibility;

(b) The Head of the ESA Security Office for Systems hosted in ESA facilities not connected with National Information Systems.

(c) a panel staffed by ESA and the appropriate NSA/DSAs, when different components of a System fall under the competence of ESA and ESA Member States.

18. The SAA shall be responsible for the following tasks:

(a) ensuring that the System complies with the relevant security policies and security guidelines, providing a statement of approval for it to handle Classified Information to a defined level of classification in its operational environment, stating the terms and conditions of the accreditation, and the criteria under which re-approval is required;

(b) establishing a security accreditation process, in accordance with the relevant policies, clearly stating the approval conditions for the System under its authority;

(c) defining a security accreditation strategy setting out the degree of detail for the accreditation process commensurate with the required level of assurance;

(d) examining and approving security-related documentation, including risk management and residual risk statements, and statement of compliance;

(e) checking implementation of security measures in relation to the System by undertaking or sponsoring security assessments, inspections or reviews;

(f) defining specific security requirements (e.g. personnel clearance levels) for sensitive positions in relation to the System;

(g) endorsing the selection of approved cryptographic and TEMPEST products used to provide security for the System;

(h) approving, or where relevant, participating in the joint approval of the interconnection of a System to other System(s); and

(i) consulting the System provider, the security actors and representatives of the users with respect to security risk management, in particular the residual risk, and the terms and conditions of the approval statement.

ESA INFOSEC OFFICER

19. The ESA INFOSEC Officer is the staff of the ESA Security Office having the overall responsibility for the specification, development, and implementation of a security system or network. The responsibility for the development and implementation can be delegated to the appropriate ESA service in order to ensure proper operations.

ESA TEMPEST OFFICER

20. The ESA TEMPEST Officer shall be responsible for ensuring compliance of a System with TEMPEST policies and guidelines. He shall approve TEMPEST countermeasures for installations and products to protect Classified Information to a defined level of classification in its operational environment.

ESA CRYPTO APPROVAL OFFICER

21. The ESA Crypto Approval Officer shall be responsible for ensuring that cryptographic products comply with ESA or National cryptographic security policy. He shall advise the SAA on the selection of a cryptographic product to protect Classified Information to a defined level in its operational environment.

ESA CRYPTO DISTRIBUTION OFFICER

22. The ESA Crypto Distribution Officer shall be responsible for:

    (a) managing and accounting for ESA cryptographic material;

    (b) ensuring that appropriate procedures are enforced and channels established for accounting, secure handling, storage and distribution of all ESA crypto material; and

    (c) ensuring the secure transfer of ESA crypto material to or from individuals or services using it.

IT SYSTEM OPERATIONAL AUTHORITY (ITSOA) AND PROJECT/SYSTEM SECURITY OFFICER (PSSO)

23. The INFOSEC Officer shall delegate at the earliest stage possible the responsibility for the implementation and operation of controls and special security features of the System to the ESA IT System Operational Authority (ITSOA) at the corporate level or to the security officer of that specific System, the Project/System Security Officer (PSSO), as appropriate. This responsibility shall extend throughout the life cycle of the System from the project concept stage to final disposal.

24. The ITSOA/PSSO shall be responsible for all security measures designed as part of the overall System. This responsibility includes producing the SECOPS. The ITSOA/PSSO shall specify the security standards and practices to be met by the supplier of the System.

USERS

25. All users, in accordance with the provisions of Section V, shall be responsible for ensuring that their actions do not adversely affect the security of the System that they are using.

TRAINING

26. Awareness of the risks and available security measures is the first line of defence for the security of Information Systems. Education and training on usage of IT Systems shall be made available by the ESA INFOSEC Officer at various levels, within ESA facilities. In particular, all personnel involved in the life-cycle of a System, including users, shall understand:

    (a) that security failures may significantly harm and compromise the system, in part or in its entirety;

    (b) the potential harm to others which may arise from interconnectivity and interdependency; and

    (c) their individual responsibility and accountability for the security of the system according to their roles.

IT SECURITY MEASURES APPLICABLE TO PERSONNEL

27. Users requiring access to certain equipment or information specific to security of systems (like, e.g., cryptographic equipment) will be subject to a special clearance issued according to specific existing national regulations.

28. The competent security authority shall determine all sensitive positions and specify the level of clearance and supervision required by all personnel occupying them, taking into account of the effects of aggregation where appropriate.

29. Systems shall be specified and designed in a way that facilitates the allocation of duties and responsibilities to personnel so as to prevent one single person having complete knowledge or control of the system security key points (two-men rule).

PHYSICAL SECURITY APPLICABLE TO IT SYSTEMS

30. IT and remote workstations in which information classified ESA CONFIDENTIAL and above is handled by IT systems, or where potential access to such information is possible, shall be established as ESA Class I or Class II security areas or national equivalent, as defined in Section III.

CONTROL OF ACCESS TO AN IT SYSTEM

31. All information and material which allow access control to a system shall be protected under arrangements commensurate with the highest classification and the category designation of the information to which it may give access.

32. When no longer used for this purpose, the access control information and material shall be retained in accordance with SAA procedures and/or national regulations. Their eventual destruction shall be performed pursuant to paragraphs 39 to 41 below.

SECURITY OF INFORMATION IN AN IT SYSTEM

33. The responsible PSSO, in consultancy with the ESA Security Office shall consider the problems of aggregation of individual elements of information, and the inferences that can be gained from the related elements, and determine whether or not a higher classification is appropriate to the totality of the information. For example, large volumes of information classified ESA RESTRICTED may warrant an ESA CONFIDENTIAL marking. The same considerations shall apply to information held on portable computing devices.

34. In accordance with Section IV, when information is transferred from one system to another the information shall be protected during transfer and in the receiving system in a manner commensurate with the classification of the information.

35. In accordance with Section IV, all computer storage media shall be handled in a manner commensurate with the highest classification of the stored information or the media label, and at all times shall be appropriately protected.

36. In accordance with Section IV, reusable computer storage media used for recording Classified Information shall retain the highest classification for which they have ever been used until that information has been properly downgraded or declassified and the media reclassified accordingly, or the media declassified or destroyed in accordance with a procedure approved by the SAA (see paragraphs 39 to 41 below).

TRACEABILITY OF INFORMATION IN IT SYSTEMS

37. Automatic (audit trails) or manual logs shall be kept as a record of access to information classified ESA CONFIDENTIAL and above and regularly reviewed by appropriately security cleared and trained personnel. These records shall be retained in accordance with these Regulations.

HANDLING AND CONTROL OF REMOVABLE COMPUTER STORAGE MEDIA

38. All removable computer storage media containing Classified Information shall be handled as classified material, marked with clearly recognizable identification and appropriate classification markings, adapted to the specific physical appearances of the media, unless the information is encrypted as described in paragraph 47 below.

DOWNGRADING AND DESTRUCTION OF COMPUTER STORAGE MEDIA

39. Computer storage media used for recording Classified Information may be downgraded or destroyed in accordance with methods and procedures approved by the competent security authority.

40. Computer storage media, which have held information classified ESA CONFIDENTIAL shall not be downgraded (unless all files ever stored on the media have been downgraded) but may be reused at the same level.

41. Computer storage media, which have held ESA SECRET and above information shall not be downgraded and reused.

SECURITY OF ELECTRONIC TRANSMISSIONS

42. The direct connection of two or more systems handling information classified ESA CONFIDENTIAL and above (i.e. interconnection) for the purpose of sharing information shall be implemented with protective measures to control the exchange of Classified Information, approved by the SAA on the basis of a specific SISRS (System Interconnection Security Requirement Statement) according to provisions for accreditation of IT systems as specified in this Section.

43. For transmission of information classified ESA RESTRICTED, the provisions of paragraphs 12 to 14 above shall apply.

44. There shall be no interconnection between an accredited system and an unprotected or public network, except where the system has an approved boundary protection system installed for such a purpose between the system and the unprotected or public network. The security measures for such interconnections shall be reviewed by the ESA INFOSEC Officer and approved by the SAA.

45. The direct or cascaded interconnection of a system accredited to handle ESA TOP SECRET to an unprotected or public network shall be prohibited.

46. When an unprotected or public network is used solely as a carrier and the data is encrypted by a cryptographic product approved in accordance with paragraph 47 of this Section, such a connection shall not be deemed to be an interconnection, whilst availability still needs to be addressed.

47. Cryptographic products used to provide confidentiality, integrity, availability, authenticity, or non-repudiation of Classified Information shall have been evaluated and approved by the competent security authorities of two ESA Member States, subject to the availability of suitable dual-approved products. Should no such products be available, the use of products which have been approved by a single Member State is permitted subject to the provisions of paragraph 48 below.

48. The confidentiality of ESA Classified Information in CIS shall be protected by cryptographic products the use of which has been approved by the ESA Security Committee upon advice of the INFOSEC panel.

49. Under exceptional operational circumstances, information classified ESA RESTRICTED, ESA CONFIDENTIAL and ESA SECRET may be transmitted with cryptographic products approved for a lower classification level or even in clear text, provided each occasion is explicitly authorised and duly registered by the Head of the ESA Security Office. Such exceptional circumstances are as follows:

    (a) during impending or actual crisis, conflict, or war situations; and

(b) when speed of delivery is of paramount importance, and appropriate means of encryption are not available, and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations. In such cases, the Classified Information transmitted shall not bear any classification marking and the recipient shall be immediately and by other means informed of the level of classification of the information concerned.

50. A system shall have the capability of positively denying access to Classified Information at any or all of its remote workstations, when required either by physical disconnection or by special software features approved by the SAA.

TEMPEST SECURITY

51. Initial installation of systems and any change thereto shall be carried out by technically qualified personnel who are security cleared for access to Classified Information to a level equivalent to the highest classification which the System is expected to store and handle.

52. Systems handling information classified ESA CONFIDENTIAL and above shall be protected in such a way that their security cannot be threatened by compromising emanations, the study and control of which is referred to as “TEMPEST”.

53. TEMPEST measures for ESA shall be reviewed and approved by the ESA TEMPEST Authority.

SOFTWARE PROTECTION/CONFIGURATION MANAGEMENT

54. Security protection of applications programmes shall be determined on the basis of an assessment of the overall security classification of the programme itself rather than of the classification of the information it is to process.

55. Security of software has to be ensured throughout its lifecycle: The software versions in use shall be verified at regular intervals to ensure their integrity and correct functioning**.** Security patches shall be applied regularly as necessary.

56. Only the essential user privileges, functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risk (principle of minimalism).

57. New or modified versions of software for the handling of Classified Information shall be approved by the ITSOA/PSSO before installation. New software must in any case be approved by the SAA, as stated in the SSRS.

CHECKING FOR THE PRESENCE OF MALICIOUS SOFTWARE/COMPUTER VIRUSES

58. Checking for the presence of malicious software/computer viruses shall be carried out in accordance with the requirements of the SAA.

59. All computer storage media arriving in ESA shall be checked for the presence of any malicious software or computer viruses, automatically upon connection to any System, using tools and facilities approved by the ESA INFOSEC Officer. Automatic execution of software upon connection shall be disabled.

MAINTENANCE OF IT SYSTEMS

60. Contracts and procedures for scheduled and on-call maintenance of systems for which a SSRS has been produced shall specify requirements and arrangements for maintenance personnel and their associated equipment accessing an IT area.

61. The requirements shall be clearly stated in the SSRS and the procedures shall be clearly stated in the SECOPS. Contractor maintenance requiring remote access diagnostic procedures shall be permitted only in exceptional circumstances, under stringent security control, and only with the approval of the SAA.

ACCREDITATION OF IT SYSTEMS

62. All systems handling Classified Information shall be subject to prior accreditation by the competent security authority based on the SSRS. However, for systems handling only information at the level of ESA RESTRICTED, the accreditation process can follow a lightweight path. Other systems may be subject to accreditation according to their specific security and business needs.

63. Systems operated by ESA Member States' public or private facilities will be accredited by the competent NSA/DSA. Systems operated by ESA itself and which are not connected to systems operated by ESA Member States' public or private facilities will be accredited by the ESA SAA. Systems operated by ESA connected to ESA Member States' public or private facilities will be accredited by a joint panel of representatives of the NSA's/DSA's of the ESA Member States concerned and ESA SAA.

64. The accreditation process will be carried out in accordance with a security accreditation strategy appropriate to the particular system and defined by the SAA, that will also address the statement of compliance with the SSRS and the accreditation certificate stating the maximum classification level of the information that can be handled as well as the corresponding terms and conditions, including the duration.

65. For all systems handling Classified Information, a System-specific Security Requirements Statement (SSRS) or System Interconnection Security Requirement Statement (SISRS) shall be produced by the IT System Operational Authority (ITSOA)/its Project/System Security Officer (PSSO) in cooperation with input and assistance as required from the project staff and the INFOSEC Officer, and approved by the Security Accreditation Authority (SAA).

66. The SSRS/SISRS shall be formulated at the earliest stage of an IT project's inception and shall be developed and enhanced as the project develops, fulfilling different roles at different stages in the project and system's life cycle.

67. The SSRS/SISRS shall form the binding agreement between the IT System Operational Authority/Technical System Owner and the Information Owner and the SAA by which the system is to be accredited.

68. The SSRS/SISRS is a complete and explicit statement of the security principles to be observed and of the detailed security requirements to be met. It is based on ESA Security Regulations and risk assessment and takes into account the operational environment, the security mode of operation, and any specific user requirements. The SSRS/SISRS is an integral part of project documentation submitted to the appropriate authorities for technical, budgetary and security approval purposes. In its final form, it constitutes a complete statement of what it means for the system to be secure.

69. The Security Operating Procedures (SECOPS) of the specific system define the objectives of a security system in relation to the SSRS/SISRS, the adopted solutions, the operating procedures to be followed to achieve the goals of the SSRS/SISRS, and the responsibilities of related personnel. The SECOPS shall be prepared under the responsibility of the ITSOA/PSSO.

CERTIFICATION OF IT SYSTEMS

70. Any security product (except cryptographic products) to be used by an ESA IT system shall be certified against internationally acknowledged criteria (such as the Common Criteria for Information Technology Security Evaluation, ISO 15 408).

71. Where appropriate, the requirements for certification shall be included in system planning, and clearly stated in the SSRS.

72. For cryptographic products the applicable provisions are described in paragraph 47 above.

73. The degree of certification processes involved may be simplified (e.g., only involving integration aspects) where IT systems are based on existing certified computer security products.

ROUTINE CHECKING OF SECURITY FEATURES FOR CONTINUED ACCREDITATION

74. The ITSOA/PSSO shall establish routine control procedures to ensure that all security features of the system are still valid.

75. The types of change that would give rise to re-accreditation, or that require the prior approval of the SAA, shall be clearly identified and stated in the SSRS. After any modification, repair or failure, which could have affected the security features of the System, the ITSOA/PSSO shall ensure that a check is made to ensure the correct operation of the security features. Continued accreditation of the system shall normally depend on the satisfactory completion of the checks.

76. All systems where security features have been implemented shall be inspected or reviewed on a periodic basis by the SAA. In respect of systems handling ESA TOP SECRET or additional markings information, the inspections shall be carried out not less than once annually.

SECURITY OF PORTABLE COMPUTING DEVICES

77. Hard disks of portable computing devices (e.g. portable PCs, smartphones, notebooks, etc.) shall be considered as information storage media in the same sense as any other removable computer storage media (e.g. USB memory sticks or external hard disks) as addressed in paragraphs 38 to 41 above.

78. This equipment shall be afforded the level of protection, in terms of access, handling, storage and transportation, commensurate with the highest classification level of information ever stored or processed on them (until downgraded or declassified in accordance with approved procedures).

79. The use of privately-owned computer storage media, software and IT hardware (e.g. PCs, laptops, smartphones, USB memory sticks) with storage capability shall be prohibited for handling Classified Information.

SECURITY OF IT EQUIPMENT NOT OWNED BY ESA

80. The use of IT equipment and software not owned by ESA operated in support of official ESA work may be permitted by the Head of the ESA Security Office. In this case, the IT equipment shall be brought under the control of the appropriate ESA's inventory and configuration control. If such IT equipment is to be used for handling Classified Information, then the SAA shall be consulted in order that the elements of information assurance that are applicable to the use of that equipment are properly considered and implemented.

SECTION VII - INDUSTRIAL SECURITY

This Section sets out the provisions for implementing the security measures related to industrial activities that are unique to the negotiation and placing of ESA classified contracts (i.e. contracts involving Classified Information) throughout the life-cycle of the classified contract, including the release during the bidding period, pre-contract negotiations and access to, handling, storage of Classified Information.

PROGRAMME / PROJECT SECURITY INSTRUCTION (PSI)

1. Depending on the scope of programmes or projects involving access to or handling or storage of Classified Information, specific Programme/Project Security Instructions (PSI) shall be drafted by the ESA Security Office in co-operation with the ESA programme and procurement authorities designated to manage the programme or project.

2. The specific PSI shall be based upon the ESA Generic PSI. The ESA Security Office shall be the custodian of the document.

3. The specific PSI, completed with its Security Classification Guide, shall be defined and approved by the ESA Security Committee and the Participating States of the ESA Programme concerned. It will be annexed to the corresponding ESA classified contract, and will form an integral part of the contract or sub-contract.

4. The specific PSI, including the Security Classification Guide, shall be referred to in the Implementing Rules of the programme concerned. Once the Implementing Rules are approved by the ESA Council, the approval process for the classified contracts will be applied to the protected programme elements concerned.

5. The Security Classification Guide shall identify the security marking of any information to be provided to potential bidders and contractors, as well as any information that may be created by the contractor.

6. In order to determine the security classification of the various elements of a classified contract, the following principles shall apply:

   (a) in preparing a Security Classification Guide, the ESA Security Office and ESA programme and procurement authorities shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract by the originator of the information;

   (b) the overall level of classification of the contract may not be lower than the highest classification of any of its elements;

   (c) The originator should regularly check whether any of the relevant Classified Information should be reclassified; and

(d) where relevant, ESA shall liaise with the originator concerned in the event of any changes regarding the classification of information created by or provided to contractors in the performance of a contract and when making any subsequent changes to the Security Classification Guide.

7. The ESA Security Office, in co-operation with the ESA programmatic and procurement authorities designated to manage the programme or project and the relevant NSA(s) or DSA(s) if necessary, is responsible for maintaining and updating the annexes of the specific Programme/Project Security Instructions.

8. The PSI shall contain the provisions requiring the contractor and/or subcontractor to comply with the minimum standards laid down in these Regulations. It shall also contain a provision that notwithstanding possible legal consequences following a security breach or compromise of information, non-compliance with these minimum standards may constitute grounds for the contract to be terminated with fault of the contractor.

SECURITY ASPECTS LETTER (SAL)

9. Contract-specific security requirements may be described in a Security Aspects Letter (SAL):

(a) to address specific contractual security details which are not contained in, or addressed by a PSI; or

(b) to replace a PSI if it is deemed more appropriate and practical (for instance in the case where only certain sections of the PSI would be applicable to a contract). In this case, the SAL shall, where appropriate, contain the Security Classification Guide (see paragraphs 3 to 5 above).

10. The SAL shall form an integral part of a classified contract or sub-contract.

11. The SAL shall contain the provisions requiring the contractor and/or subcontractor to comply with the minimum standards laid down in these Regulations. It shall also contain a provision that notwithstanding possible legal consequences following a security breach or compromise of information, non-compliance with these minimum standards may constitute grounds for the contract to be terminated with fault of the contractor.

FACILITY SECURITY CLEARANCE (FSC)

12. A Facility Security Clearance (FSC) shall be granted by the NSA, DSA or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an entity can protect Classified Information at the appropriate classification level within its facilities. It shall be presented to ESA, as the contracting authority, before a contractor or potential tenderer may be provided with or granted access to Classified Information.

13. When issuing an FSC, the relevant NSA or DSA shall, as a minimum:

    (a) evaluate the integrity of the entity;

    (b) evaluate ownership, control, or the potential for undue influence that may be considered a security risk;

    (c) verify that the entity has established a security system at its facility which covers all appropriate security measures necessary for the protection of information or material classified ESA CONFIDENTIAL or above in accordance with the requirements laid down in these Regulations;

    (d) verify that the management, owners and employees who need to have access to information classified ESA CONFIDENTIAL or above have a PSC in accordance with the requirements laid down in Section V;

    (e) verify that the entity has appointed a Facility Security Officer who is responsible to its management for enforcing the security obligations within such an entity.

14. PSCs shall be required for all contractor personnel having access to Information classified ESA CONFIDENTIAL or above either at the cleared contractor's site or at any other cleared facilities. Where relevant, the ESA Security Office shall notify the appropriate NSA/DSA in due time that an FSC or PSC is required in the pre-contractual stage or for performing the contract.

15. The contracting authority shall not award a classified contract involving information classified ESA CONFIDENTIAL or above with a recommended tenderer before having received confirmation from the NSA/DSA or any other competent security authority of the Member State in which the contractor concerned is located that, where required, an appropriate FSC has been issued.

16. The NSA/DSA or any other competent security authority which has issued an FSC shall notify the ESA Security Office about changes affecting contractors' FSC.

17. Withdrawal of an FSC by the relevant NSA/DSA or any other competent security authority shall constitute sufficient grounds for ESA, as the contracting authority, to terminate a classified contract, or to exclude a potential tenderer or tenderer from the competition.

PERSONNEL SECURITY CLEARANCES FOR PERSONNEL WORKING FOR CONTRACTORS

18. All personnel working for contractors requiring access to Classified Information ESA CONFIDENTIAL or above shall have been appropriately security cleared and have a need-to-know to access the information pursuant to the provisions of Section V. Although a PSC is not required for access to Classified Information at the level of ESA RESTRICTED, the need-to-know for such access shall exist.

19. Applications for the PSCs for personnel working for contractors shall be made to the NSA/DSA responsible for the entity.

20. If an entity wishes to employ a national of an ESA non-member State in a position that requires access to Classified Information, it is the responsibility of the NSA/DSA of the Member State in which the hiring entity is located and incorporated, to carry out the security clearance procedure in accordance with national laws and regulations. Access to Classified Information by this individual shall be granted in accordance with the provisions of Section V.

CLASSIFIED CONTRACTS AND SUB-CONTRACTS

21. All contracts shall contain the appropriate "ESA Security Clauses for Classified Contracts" as approved by the ESA competent service.

22. An FSC shall be required in the pre-contractual stage where information classified ESA CONFIDENTIAL or above has to be provided to the tenderer in the course of the tendering process. Before entering into negotiations of a prime contract with a tenderer concerning information classified ESA CONFIDENTIAL or above, the ESA Security Office shall inform the NSA/DSA concerned using the Facility Security Information Sheet (FIS, a template of which is attached in Annex 5 attached thereto).

23. Once a classified contract has been awarded, ESA, as contracting authority, shall notify the contractors' NSA/DSA or any other competent security authority, on the security provisions of the classified contract.

24. Classified contracts shall contain provisions that bind the contractors, under penalty of termination of their contract for fault, to take all measures prescribed by ESA and/or NSAs/DSAs respectively for safeguarding all Classified Information generated by or entrusted to the contractors in accordance with the respective PSI or SAL.

25. At whatever level it is proposed to tender for or to negotiate a sub-contract, the following shall apply:

    (a) Before entering into negotiations of a sub-contract concerning information classified ESA CONFIDENTIAL or above, the Security Officer of the contractor having issued the invitation to tender shall request via his NSA/DSA the relevant NSA/DSA for confirmation that the potential sub-contractor holds an appropriate FSC to protect Classified Information. Where the potential sub-contractor does not hold the required FSC, the NSA/DSA of the contractor having issued the invitation to tender shall notify the appropriate NSA/DSA;

    (b) NSA/DSA of the potential sub-contractor will return the completed form together with the required information to the contractor, following the same channels;

(c) Upon receipt of the assurance that the proposed sub-contractor holds a FSC or provisional FSC to the required level the contractor may open negotiations with the potential sub-contractor. It remains the responsibility of the NSA/DSA of the sub-contractor to make the appropriate arrangements to ensure the protection of all Classified Information issued to the latter.

26. The conditions under which the contractor may subcontract shall be defined in the invitation to tender and in the contract.

27. A contractor shall obtain permission from ESA, as the contracting authority, before sub-contracting any parts of a classified contract. No sub-contract may be awarded to entities registered in an ESA non-member State which have not concluded a Security Agreement with ESA.

28. The contractor shall be responsible for ensuring that all sub-contracting activities are undertaken in accordance with the minimum standards laid down in these Regulations and shall not provide Classified Information to a subcontractor without the prior written consent of ESA as the contracting authority.

29. With regard to Classified Information created or handled by a contractor, the rights incumbent on the originator shall be exercised by ESA as the contracting authority.

NON-AWARDING, COMPLETION OR TERMINATION OF CLASSIFIED CONTRACTS OR SUB-CONTRACTS

30. Where Classified Information is provided to an entity at the pre-contractual stage, the invitation to tender shall contain a provision obliging the potential tenderer which fails to submit an offer, or the tenderer which is not selected to return all classified documents within a specified period of time. In case a tenderer fails to do so, the relevant NSA/DSA shall be informed.

31. When such contracts are completed or terminated, ESA, as contracting authority, (and/or the NSA/DSA or any other competent security authority, as appropriate, in the case of a sub-contract) shall promptly notify the NSA/DSA or any other competent security authority of the Member State in which the contractor is registered.

32. As a general rule, a contractor shall be required to return to the contracting authority, upon completion or termination of the classified contract or sub-contract, any Classified Information held by it.

33. Specific provisions for the disposal of Classified Information during the performance of the contract or upon its completion or termination shall be laid down in the PSI or SAL.

34. Where the contractor is authorised to retain Classified Information after completion or termination of a contract, the minimum standards contained in

these Regulations shall continue to be complied with and the confidentiality of Classified Information shall be protected by the contractor.

VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

35. Where ESA and contractors need access to information classified ESA CONFIDENTIAL or above in each other's premises for the performance of a classified contract, visits shall be arranged in liaison and agreement with the NSA/DSA or any other competent security authority concerned. However, in the context of specific programmes/projects, the NSAs/DSAs may also agree on a procedure whereby such visits can be arranged directly.

36. All visitors shall hold an appropriate PSC and have a "need-to-know" for access to the Classified Information related to the contract.

37. Visitors shall be given access only to Classified Information related to the purpose of the visit.

38. International visits involving access to information classified ESA CONFIDENTIAL or above are based on the use of the "Request for Visit" (RFV) procedure (form shown in Annex 6 attached hereafter).

39. Requests for recurring visits shall normally be used for contracts for all ESA programmes. They shall have a maximum validity of one year from the start date requested in the RFV. The requests shall be re-submitted for re-issuance, when necessary.

40. Visits relating to information classified ESA RESTRICTED shall be arranged directly between the sending facility and the facility to be visited.

TRANSMISSION AND CARRIAGE OF CLASSIFIED INFORMATION

41. As a general rule, the preferred procedure is that Classified Information shall be transmitted by electronic means protected by cryptographic products approved in accordance with Section VI;

42. With regard to the transmission of Classified Information, the relevant provisions of Section IV shall apply, in accordance with national laws and regulations.

43. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:

    (a) security shall be assured at all stages during transportation from the point of origin to the final destination;

    (b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;

(c) a FSC where appropriate, shall be obtained for companies providing transportation. In such cases, personnel handling the consignment shall be appropriately security cleared in accordance with Section V;

(d) prior to any cross-border movement of material classified ESA CONFIDENTIAL or above, a transportation plan shall be drawn up by the consignor and approved by the NSA/DSA of both the consigner and the consignee or any other competent security authority concerned;

(e) journeys shall be point-to-point to the extent possible, and shall be completed as quickly as circumstances permit;

(f) whenever possible, routes shall be only through ESA Member States. Routes through States other than ESA Member States shall only be undertaken when authorised by the ESA Security Office and the involved ESA Member States.

TRANSPORTATION OF ITEMS CLASSIFIED ESA CONFIDENTIAL OR ESA SECRET BY COMMERCIAL CARRIERS AS FREIGHT

44. Classified items that cannot be transmitted by one of the foregoing methods or where large volumes of classified material (e.g. equipment, components of satellites or launchers) are to be conveyed, they may be transported as freight by commercial carriers in line with the following criteria for handling international shipment, as appropriate. The concerned commercial carrier shall:

(a) ensure that the personnel handling the consignment is appropriately security cleared by an ESA Member State;

(b) be authorised by laws or regulations of the ESA Member State of origin to provide international transportation services; and

(c) have the obligation to comply with safety, security and emergency procedures which must be observed.

TRANSPORTATION BY ROAD OF CLASSIFIED FREIGHT

45. The following standards shall be applied when consignments of classified material are transmitted by road transportation:

(a) the carrier, the driver and/or co-driver must be security cleared up to the level of the classification of the consignment;

(b) the material will be adequately secured in vehicles or containers with a lock or padlock which is to be sealed;

(c) containers must bear no visible indication of their contents;

(d) consignments will be transported point-to-point;

(e) consignments classified ESA CONFIDENTIAL or above shall be accompanied by security personnel; this task can be performed by the driver and/or co-driver, provided they are adequately trained.

(f) security personnel having/requiring access or potential access to the Classified Information shall be appropriately cleared;

(g) during stops the consignment shall be guarded;

(h) the consignor and the consignee are responsible for jointly organising the transport and shall, in the case of consignments classified ESA CONFIDENTIAL or above, notify their respective NSA/DSA or any other competent security authority who shall jointly approve the transportation plan;

(i) where appropriate, the NSAs/DSAs or any other competent security authority will advise their customs or other relevant national authorities of impending consignments and shall be urged to give maximum priority to the shipment; and

(j) loading and unloading shall be under security control.

TRANSPORTATION BY RAIL OF CLASSIFIED FREIGHT

46. Transportation by rail may be used for consignments of classified material on the basis of the following conditions:

(a) the material will be adequately secured in the train car or in a container with a lock or padlock which is to be sealed;

(b) containers must bear no visible indication of their contents;

(c) during stops the consignment shall be guarded;

(d) consignments classified ESA CONFIDENTIAL or above shall be accompanied by security personnel;

(e) security personnel having/requiring access or potential access to the Classified Information shall be appropriately security cleared;

(f) the consignor and the consignee are responsible for jointly organising the transport and shall, in the case of consignments classified ESA CONFIDENTIAL or above, notify their respective NSA/DSA or any other competent security authority who shall jointly approve the transportation plan;

(g) where appropriate, the NSAs/DSAs or any other competent security authority will advise their customs or other relevant national authorities of impending consignments and shall be urged to give maximum priority to the shipment;

(h) loading and unloading shall be under security control; and

(i) delivery of the consignment to the station of departure and collection from the station of destination must be so timed to prevent, as far as possible, a consignment being held in at the station.

TRANSPORTATION BY SEA OF CLASSIFIED FREIGHT

47. The following standards shall be applied when consignments of ESA material classified ESA CONFIDENTIAL or above are sent by sea:

(a) the material will be adequately secured in vehicles or containers with a lock or padlock which is to be sealed;

(b) containers must bear no visible indication of their contents;

(c) preferably the consignment shall be stowed in locked stowage space approved by the NSA/DSA of the consignor;

(d) consignments classified ESA CONFIDENTIAL or above shall be accompanied by security personnel;

(e) security personnel having/requiring access or potential access to the Classified Information shall be appropriately security cleared;

(f) consignments classified ESA CONFIDENTIAL or above shall be guarded during the voyage;

(g) the consignor and the consignee are responsible for jointly organising the transport and shall, in the case of consignments classified ESA CONFIDENTIAL or above, notify their respective NSA/DSA or any other competent security authority who shall jointly approve the transportation plan;

(h) where appropriate, the NSAs/DSAs or any other competent security authority will advise their customs or other relevant national authorities of impending consignments and shall be urged to give maximum priority to the shipment.;

(i) stops at maritime countries presenting special security risks shall be assessed by the NSAs/DSAs or any other competent security authorities of the consignor and the consignee. Unless the ship is in emergencies, it shall not enter the territorial waters of any of these countries without the authorisation of the NSAs/DSAs or any other competent security authorities concerned;

(j) stops at any ESA non-member States' port shall not be permitted unless prior approval of the consignor's NSA/DSA or any other competent security authority has been obtained;

(k) loading and unloading shall be under security control; and

(l) delivery to the port of embarkation and collection from the port of disembarkation must be so timed to prevent, as far as possible, a consignment being held in port warehouses.

TRANSPORTATION BY AIRCRAFT OF CLASSIFIED FREIGHT

48. An air carrier may be used provided the following standards shall be applied:

(a) the material will be adequately secured in a container with a lock or padlock which is to be sealed;

(b) containers must bear no visible indication of their contents;

(c) during stops the consignment shall be guarded;

(d) consignments classified ESA CONFIDENTIAL or above shall be accompanied by security personnel whenever possible;

(e) security personnel having/requiring access or potential access to the Classified Information shall be appropriately security cleared;

(f) the consignor and the consignee are responsible for jointly organising the transport and shall, in the case of consignments classified ESA CONFIDENTIAL or above, notify their respective NSA/DSA or any other competent security authority who shall jointly approve the transportation plan;

(g) where appropriate, the NSAs/DSAs or any other competent security authority will advise their customs or other relevant national authorities of impending consignments and shall be urged to give maximum priority to the shipment;

(h) loading and unloading shall be under security control;

(i) delivery of the consignment to the airport of departure and collection from the airport of destination must be so timed to prevent, as far as possible, a consignment being held in at the airport;

(j) airlines of ESA Member States shall normally be used. However, in exceptional circumstances such as the extreme size of the consignment, airlines of an ESA non-member States may be used in consultation with the NSA/DSA or any other competent security authority of the consignor; and

(k) direct flights shall be used whenever possible and, except in an emergency, stops at airports in ESA non-member States shall not be permitted unless final destination is in an ESA non- member State.

SECURITY GUARDS AND ESCORTS

49. Individuals fulfilling the duties of security guards may be armed or unarmed depending on national laws and regulations and arrangements made by between the NSAs/DSAs or any other competent security authorities of the ESA Member States affected by the transportation.

50. The security guards shall be appropriately security cleared by an ESA Member State should they have or require access to consignments classified ESA CONFIDENTIAL or above.

51. The security guard/escort shall be composed of an adequate number of personnel as to ensure security, regular tours of duty and rest. Their number shall depend on the classification level of the material, the method of transportation to be used, the estimated time in transit and the quantity of material will also be considered.

52. It is the responsibility of the consignor and, where applicable, the consignee to instruct security guards in their duties. The person in charge of the security guards shall also be given a copy of "Notes for the Courier" (See Annexes 3 and 4 attached hereafter) and be required to sign a receipt for it.

TRANSFER OF CLASSIFIED INFORMATION TO CONTRACTORS LOCATED IN THIRD STATES

53. In accordance with the provisions laid down in Section IX, Classified Information shall be transferred to contractors located in third States in accordance with security measures agreed between ESA, as contracting authority, and the NSA/DSA of the concerned third State where the contractors are located.

HANDLING AND STORAGE OF INFORMATION CLASSIFIED ESA RESTRICTED

54. In liaison, as appropriate, with the NSA/DSA of the Member State, ESA, as the contracting authority, shall be entitled to conduct visits of contractors' facilities on the basis of contractual provisions in order to verify that the relevant security measures for the protection of information classified ESA RESTRICTED as required under the contract have been put in place.

55. To the extent necessary under national laws and regulations, NSAs/DSAs or any other competent security authority shall be notified by ESA as the contracting authority of contracts containing information classified ESA RESTRICTED.

56. An FSC or a PSC for contractors and their personnel shall not be required for contracts let by ESA containing information classified ESA RESTRICTED.

57. ESA, as contracting authority, shall examine the responses to invitations to tender which require access to information classified ESA RESTRICTED, notwithstanding any requirement relating to FSC or PSC which may exist under national laws and regulations.

58. The conditions under which the contractor may subcontract shall be in accordance with the provisions of this Section.

59. Where a contract involves the handling of information classified ESA RESTRICTED in a Communication and Information System (CIS) operated by a contractor, the scope of accreditation of such CIS shall be agreed between the contracting authority and the respective relevant NSA/DSA.

SECURITY BREACHES AND COMPROMISE OF CLASSIFIED INFORMATION

60. The competent security authorities of the ESA Member States will investigate all cases in which it is known or where there are grounds for suspecting that Classified Information provided to or generated by a contractor pursuant to an ESA contract has been compromised. Each NSA/DSA will comply with the investigative requirements of Section X.

SECTION VIII - BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

1. This Section sets out the provisions related to the security measures concerning business continuity planning and disaster recovery (BCDR). Its primary goals in the framework of these Regulations are the protection of Classified Information from any loss or destruction in order to ensure the restoration of normal activities and operation related to the protection of Classified Information within the shortest delays possible.

2. The ESA Security Office shall liaise with the Member States' relevant authorities concerning the status of the Agency's facilities on the Member States' territory. It shall in particular supply the necessary information to ensure the facility is acknowledged as a Critical Infrastructure where and if required in accordance with the relevant national laws and regulations of the Member State concerned, if deemed appropriate by both the ESA Member State and the ESA Security Office.

3. The ESA Security Office shall ensure that precise and specific BCDR plans are established for ESA facilities holding Classified Information. They will consist of separate emergency plans based on a specific policy for each type of disaster which has a significant probability of occurring at that specific site or location. Key items to be addressed are:

   (a) risk assessment as to the hazards involved;

   (b) emergency organisation structure;

   (c) description and details regarding emergency facilities;

   (d) listing of emergency equipment and supplies;

   (e) list of mutual aid agreements with specified entities and/or local authorities;

   (f) shut down procedures; and

   (g) evacuation procedures.

4. The ESA Security Office shall assure that copies of the plans are available at:

   (a) the concerned ESA facility holding Classified Information;

   (b) the emergency/alternate facility;

   (c) the ESA Security Office.

5. The ESA Security Office shall ensure that emergency/alternate facilities foreseen to hold Classified Information are appropriately accredited for such activities.

6. The appointed Security Officer for the relevant ESA Class I Area shall be the emergency coordinator for the protection of the Classified Information under his responsibility and for the restoration of normal activities and operation.

7. The Security Officer shall ensure that the BCDR plans are drafted in close collaboration with the relevant security and safety authorities and in line with local emergency plans.

8. The BCDR plan shall at all times foresee back-up records of the ESA Classified Information for storage at alternate facilities, whilst ensuring that the duplicate records are protected appropriately and in accordance with these Regulations.

9. For information classified ESA CONFIDENTIAL or above, the ESA Central Registry shall ensure to keep identifying records (i.e. meta-data) of all information held at this level in the Agency's registries and sub-registries and of the back-up copies thereof.

SECTION IX - EXCHANGE OF CLASSIFIED INFORMATION WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

1. This Section sets out the provisions for the exchange of Classified Information with third States and International Organisations and lays down in particular the requirements for establishing Security Agreements and Memorandums of Understanding.

FRAMEWORKS GOVERNING THE EXCHANGE OF CLASSIFIED INFORMATION

2. Where the ESA Council determines that a need exists to exchange Classified Information with a third State or an International Organisation, a Security Agreement on the exchange and protection of Classified Information shall be negotiated with the third State or International Organisation and submitted to the ESA Security Committee for recommendation to Council.

3. In the absence of a framework referred to in paragraph 2 above, a Memorandum of Understanding can be entered into in accordance with the provisions under paragraphs 19 and 20 of this Section.

4. The need to release of ESA Classified Information to third States or International Organisations will be decided by the ESA Council on the basis of:

   (a) the nature and content of such information;

   (b) the recipients' need-to-know;

   (c) the measure of advantages to ESA;

   (d) the desired degree of cooperation with the third State or International Organisation concerned;

5. Classified Information can only be released to a third State or International Organisation after receiving prior approval from the originator. If the originator can no longer be identified, the prior approval of the ESA Security Committee is required, if necessary in consultation with the appropriate ESA subordinate body.

SECURITY AGREEMENTS

6. Security Agreements shall establish the basic principles and minimum standards governing the exchange and protection of Classified Information between ESA and a third State or International Organisation. The principles and standards negotiated with the third State or International Organisation shall be no less stringent than those laid down in these Regulations. Classified Information generated under such agreements shall be ESA Classified Information.

7. Security Agreements shall provide for security implementing arrangements to be agreed between the ESA Security Office and the competent security authority of

the third State or International Organisation concerned. Such arrangements shall take account of the level of protection provided by the security regulations, structures and procedures in place in the third State or International Organisation.

8. The Security Agreements and their security implementing arrangements shall be recommended by the ESA Security Committee for adoption by the ESA Council.

9. Security Agreements shall provide that prior to the exchange of Classified Information under the agreement, the ESA Security Office shall assess and report to the ESA Security Committee that the third State or International Organisation is able to protect and safeguard Classified Information provided to it in an appropriate way and commensurate with the classification level.

10. When the ESA concludes a Security Agreement with a third State or an International Organisation, a registry shall be designated in each party as the main point of entry and exit for Classified Information exchanges.

11. Prior to the exchange of Classified Information under the agreement and implementing arrangements, the ESA Security Office shall assess and confirm in writing to the ESA Security Committee that the third State or International Organisation is deemed able to protect and safeguard information provided to it in an appropriate way, and commensurate with the classification level.

12. No Classified Information shall be exchanged by electronic means unless explicitly provided for in the Security Agreement or security implementation arrangements.

ASSESSMENT VISITS

13. In order to assess the effectiveness of the Security Regulations, structures and procedures in the third State or International Organisation concerned, assessment visits shall be conducted by the ESA Security Office and in mutual agreement with the third State or International Organisation concerned.

14. Every endeavour shall be made to conduct a full security assessment visit to the third State or International Organisation in question in order to establish the nature and effectiveness of the security systems in place before the ESA Security Committee approves the implementing arrangements. However, where this is not possible the ESA Security Committee shall receive as full a report as possible from the ESA Security Office, based on the information available to it, informing the ESA Security Committee about the security regulations applicable and the way in which security is organised in the third State or International Organisation concerned.

15. The ESA Security Committee may decide that pending examination of the outcome of an assessment visit, no Classified Information should be released, or may be released only up to a specific classification level, or else it may lay down other specific conditions governing the release of ESA Classified Information to the third State or International Organisation in question. This decision shall be

notified by the ESA Security Office to the third State or International Organisation concerned.

16. The findings of the assessment visits shall be set out in a report on the basis of which the ESA Security Committee shall determine the maximum classification level and any specific conditions governing the exchange of Classified Information with the third State or International Organisation concerned.

17. Once the Security Agreement is in force and Classified Information is exchanged with the third State or International Organisation concerned, the ESA Security Committee may decide to modify the maximum level of Classified Information which may be exchanged in paper form or by electronic means, in particular in the light of any follow-up assessment visit. The implementing arrangements may need to be amended and agreed in writing by both Parties to reflect such modifications.

18. In mutual agreement with the third State or International Organisation concerned, the ESA Security Office shall, at regular intervals, conduct follow-up assessment visits to verify that the security measures in place continue to meet the minimum standards agreed in the Security Agreement and in the implementing arrangements.

MEMORANDUMS OF UNDERSTANDING

19. Where a need exists to exchange information classified no higher than ESA RESTRICTED with a third State or International Organisation, ESA may, following a recommendation from the ESA Security Committee and according to the applicable procedure, enter into a Memorandum of Understanding or any other form of agreement with the relevant authorities of the third State or International Organisation in question. In such a case, written assurances shall be sought from the third State or International Organisation concerned to ensure that it will protect any information classified ESA RESTRICTED released to it in accordance with the basic principles and minimum standards set out in these Regulations.

20. No Classified Information shall be exchanged by electronic means unless explicitly provided for in the Memorandum of Understanding.

RELEASE OF CLASSIFIED INFORMATION TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

21. Where a framework has been established for exchanging Classified Information with a third State or International Organisation, this shall not create any obligation to exchange Classified Information to that third State or International Organisation, but only provides for an agreed legal framework to facilitate any exchanges when necessary.

22. When Classified information is to be released to a third State or International Organisation, the ESA Council will first take a decision regarding the release. When the ESA Council gives its approval to release the ESA Director General

shall authorise the actual release of the concerned Classified Information to the third State or International Organisation in question, in accordance with the principle of originator's consent and in compliance with the provisions of Section IV.

23. The ESA Director General may delegate such authorisations to the ESA Security Office.

SECTION X - SECURITY BREACHES AND COMPROMISE OF CLASSIFIED INFORMATION

1. This Section sets out the measures to be taken in the situation that a breach of security and/or compromise of Classified Information occur.

2. A breach of security occurs as the result of an act or omission contrary to ESA or national security which might endanger or compromise Classified Information.

3. Compromise of Classified Information occurs when it is lost or has wholly or in part fallen into hands of unauthorised persons, i.e. those who do not have either the appropriate security clearance or the necessary need-to-know or if there is the likelihood of such an event having occurred. Classified Information may be compromised as a result of an intentional or an unintentional act or omission.

4. All persons who are required to handle Classified Information shall be aware of the importance of reporting any actual or suspected breach of security immediately to the competent security authority within ESA or of the ESA Member State in which they are employed.

5. Where it is known or where there are reasonable grounds to assume that a breach of security has occurred resulting in Classified Information being compromised or potentially compromised, the competent security authority shall take all appropriate measures in accordance with the relevant laws and regulations to:

   (a) assess and minimise the damage done;

   (b) prevent a reoccurrence;

   (c) safeguard evidence;

   (d) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts;

   (e) notify the appropriate authorities of the effects of the breach of security and of any action taken; and

   (f) inform the originator.

6. When notifying the appropriate authorities of the effects of the breach of security, the following information shall be provided (as a minimum):

   (a) a description of the information involved, including its classification, reference and copy number (if any), date, originator, subject and scope;

   (b) a brief description of the circumstances of the breach of security, including the date, time/period during which the information was actually or suspected of being exposed to compromise; and

(c) a statement whether the originator was informed.

7. For ESA, it shall be the duty of the competent security authority, as soon as it is notified that such a breach of security may have occurred, to report the incident immediately to the ESA Security Office.

8. In the event of a suspected or actual compromise of Classified Information occurring within the jurisdiction of an ESA Member State, the competent security authority shall report this to the ESA Security Office as specified in paragraphs 6 and 7 above, through the NSA/DSA concerned.

9. Cases involving information classified ESA RESTRICTED need to be reported to the ESA Security Office only when they represent suspicious circumstances or represent a risk of future breaches/compromise.

10. On being informed that a breach of security has occurred, resulting in the compromise or potential compromise of Classified Information, the ESA Director General shall:

(a) notify the competent security authority that originated the Classified Information in question;

(b) ask the appropriate competent security authorities to initiate investigations;

(c) coordinate enquiries where more than one competent security authority is affected; and

(d) obtain a report on the circumstances of the breach in line with paragraph 7 of this Section.

11. Should there be a breach/compromise the originating authority of the Classified Information shall inform the recipients of the concerned Classified Information and shall give appropriate instructions.

12. Any individual who, after an investigation, is found to be responsible for a breach of security resulting in a compromise of Classified Information may be liable to appropriate disciplinary or legal action.

13. ESA Staff members, ESA experts and ESA contractors' employees shall be informed about the possible legal consequences of breaches of security. In particular, in the case of ESA Staff members and ESA experts, the ESA Director General shall have the duty to waive the immunity, in compliance with Article 7 of the ESA Security Agreement and Article XXI, paragraphs 1 and 2 of the Annex I to the ESA Convention.

ANNEX 1

GLOSSARY

In the context, and for the purpose of these Regulations, the following terms or expressions shall be meant as follows:

ACCREDITATION means: the process leading to a formal statement by the Security Accreditation Authority (SAA) that a system is approved to operate with a defined level of classification, in a particular security mode in its operational environment and at an acceptable level of risk, based on the premise that an approved set of technical, physical, organisational and procedural security measures has been implemented.

APPROVAL OF A CRYPTOGRAPHIC PRODUCT FOR USE means: formal process intended to determine if a product meets minimum specified standards.

AUTHORISATION TO ACCESS CLASSIFIED INFORMATION (AACI) means: a certificate issued by the ESA Security Office establishing that an ESA employee is appropriately security cleared and holds a valid national PSC and which shows the level of ESA Classified Information to which that individual is granted access (CONFIDENTIAL or above), the date of validity of the relevant AACI and the date of expiry of the certificate itself.

CERTIFICATION means: the formal confirmation of certain security characteristics of a system, a facility, or material's established suitability for a specified purpose.

CLASSIFICATION GUIDE means: the part of the Programme Security Instruction (PSI) or Security Aspects Letter (SAL), which identifies the elements of the programme/project or contract that are classified, specifying the security classification levels. The classification guide may be expanded throughout the programme life cycle, and the elements of information may be re-classified or declassified.

CLASSIFIED CONTRACT means: a contract entered into for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or the creation of Classified Information.

COMPUTER SECURITY (COMPUSEC) means: the application of hardware, firmware and software security features to a computer system in order to protect against, or to prevent the loss of integrity or availability of the systems themselves, the unauthorised disclosure, manipulation, modification/deletion of information or denial of service.

COMPUTER SECURITY PRODUCT means: a generic computer security item which is intended for incorporation into an IT System for use in enhancing, or

providing for, confidentiality, integrity, availability, authenticity, or non-repudiation of information handled.

COMMUNICATIONS SECURITY (COMSEC) means: the application of security measures to telecommunications in order to deny unauthorised persons information of value which might be derived from the possession and study of such telecommunications or to ensure the authenticity, confidentiality or integrity of such telecommunications.

COMPETENT SECURITY AUTHORITY (CSA) means: a Government authority subordinate to the National Security Authority or the prime Security Authority of an International Organisation which is responsible for implementing the security requirements covered by these Regulations.

CONTRACTOR means: an individual or legal entity possessing the legal capacity to undertake contracts agreeing to supply goods or services to ESA whether as prime or single contractor or as subcontractor.

CRYPTOGRAPHIC (CRYPTO) MATERIAL means: cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material.

DECLASSIFICATION means: the removal of any security classification.

DEFENCE IN DEPTH means: the application of a range of security measures organised as multiple layers of defence.

DESIGNATED SECURITY AUTHORITY (DSA) means: an authority responsible to the National Security Authority (NSA) of a Member State which is responsible inter alia for communicating to industry the national policy in all matters of ESA industrial security policy and for providing direction and assistance in its implementation. In some countries, the function of a DSA may be carried out by the NSA.

DOCUMENT means: any recorded information regardless of its physical form or characteristics.

DOWNGRADING means: a reduction in the level of security classification.

ENTITY means: any legal person or body.

ESA MEMBER STATE means: a State which is Party to the Convention of the European Space Agency in accordance with Articles XX and XXII of the said Convention.

ESA SECURITY AGREEMENT means: the Agreement between the State Parties to the Convention for the establishment of a European Space Agency and the European Space Agency for the protection and exchange of Classified Information approved by the ESA Council on 13 June 2002.

ESA STAFF MEMBER means: a person appointed pursuant to Article XII.3 of the ESA Convention and whose terms of employment are governed by the ESA Staff Regulations, Rules and Instructions.

FACILITY SECURITY CLEARANCE means: an administrative determination by a NSA/DSA that, from a security point of view, a facility can afford adequate security protection to ESA Classified Information of a specified classification or below, and its personnel who require access to ESA Classified Information have been properly cleared and briefed on ESA security requirements necessary to perform on the ESA classified contracts.

INFOSEC means: the application of security measures to protect information processed, stored or transmitted in Information Technology and Communications Systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the Systems themselves.

INFORMATION TECHNOLOGY SYSTEM OPERATIONAL AUTHORITY (ITSOA) means***:*** the entity responsible for the design, development, implementation, procurement, and operations of the ESA corporate IT Systems and networks, available to all ESA users.

INVITATION TO TENDER means: a formal communication to entities containing the conditions for submission together with specifications and requirements and inviting them to submit tenders for a classified contract.

IT SYSTEM means: a set of equipment, software, applications, methods and procedures, and personnel, organised to accomplish information processing functions under the same responsibility.

MATERIAL means: any document or item of machinery or equipment, either manufactured or in the process of manufacture.

NATIONAL SECURITY AUTHORITY (NSA) means: the government authority in a Member State with responsibility for the security of Classified Information covered by these Regulations.

NEED-TO-KNOW means: the principle according to which a positive determination is made by the originator that a prospective recipient has a requirement for access to, knowledge of, or possession on information in order to perform official tasks or services.

ORIGINATOR means: ESA, the ESA Member States, a third State or International Organisation under whose authority Classified Information has been created and/or introduced into ESA and its Member States.

PERSONNEL SECURITY CLEARANCE means: a statement by a competent security authority of an ESA Member State which is made following completion of a security investigation conducted by the competent security authorities of an ESA Member State and which certifies that an individual may, provided his "Need-to-Know" has been determined, be granted access to Classified Information up to a specified level (CONFIDENTIAL or above), until a specified date; the individual thus described is said to be "security cleared".

POTENTIAL TENDERER means: an entity who has registered with the Agency.

PROGRAMME/PROJECT SECURITY INSTRUCTION (PSI) means: a compilation of security regulations/procedures, which are applied to a specified programme or project in order to standardise security procedures. The PSI also constitutes an Annex to the main contract, and may be revised throughout the programme/project lifecycle.

PROJECT/SYSTEM SECURITY OFFICER (PSSO) means: the security officer of a specific project or system, responsible for the security thereof. He/she can often be identified as the Facility security officer.

SECURITY MODES OF OPERATION can be one of:

- ***DEDICATED SECURITY MODE OF OPERATION*** means: a mode of operation in which ALL individuals with access to the system are cleared to the highest classification level of information handled within the system, and have a common need-to-know for ALL of the information handled within the system;

- ***SYSTEM HIGH SECURITY MODE OF OPERATION*** means: a mode of operation in which ALL individuals with access to the system are cleared to the highest classification level of information handled within the system, but NOT ALL individuals with access to the system have a common need-to-know for the information handled within the system;

- ***MULTI-LEVEL SECURITY MODE OF OPERATION*** means: a mode of operation in which NOT ALL individuals with access to the

system are cleared to the highest classification level of information handled within the system, and NOT ALL individuals with access to the system have a common need-to-know for the information handled within the system.

TEMPEST means: the investigation, study and control of compromising electromagnetic emanations and the measures to suppress them.

TENDER means: a submission in response to an Invitation to Tender (ITT) from ESA which is intended to form the basis of a classified contract.

TENDERER means: an entity who has submitted a tender in response to an Invitation to Tender.

THIRD STATE means: any non-member State of the European Space Agency.

ANNEX 2

EQUIVALENCE TABLE FOR CLASSIFICATION MARKINGS

ESA	ESA TOP SECRET	ESA SECRET	ESA CONFIDENTIAL	ESA RESTRICTED
AUSTRIA	STRENG GEHEIM	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
BELGIUM	TRÈS SECRET (Loi 11.12.1998) ZEER GEHEIM (Wet 11.12.1998)	SECRET (Loi 11.12.1998) GEHEIM (Wet 11.12.1998)	CONFIDENTIEL (Loi 11.12.1998) VERTROUWELIJK (Wet 11.12.1998)	(Note 1, see below)
CZECH REPUBLIC	Přísně tajné	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
DENMARK	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
FINLAND	ERITTÄIN SALAINEN or YTTERST HEMLIG	SALAINEN or HEMLIG	LUOTTAMUKSELLINEN or KONFIDENTIELL	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG
FRANCE	TRES SECRET DEFENSE	SECRET DEFENSE	CONFIDENTIEL DEFENSE	(Note 2, see below)
GERMANY	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	VS-NUR FÜR DEN DIENSTGEBRAUCH
GREECE	Άκρως Απόρρητον	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
IRELAND	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
ITALY	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
LUXEMBOURG	TRES SECRET LUX	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
THE NETHERLANDS	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
NORWAY	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
PORTUGAL	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
SPAIN	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSION LIMITADA

SWEDEN	KVALIFICERAT HEMLIG or HEMLIG / TOP SECRET	HEMLIG / SECRET or HEMLIG	HEMLIG / CONFIDENTIAL Or HEMLIG	HEMLIG / RESTRICTED Or HEMLIG
SWITZERLAND		SECRET / GEHEIM / SEGRETO	CONFIDENTIEL / VERTRAULICH / CONFIDENZIALE	INTERNE / INTERN / AD USO INTERNO
THE UNITED KINGDOM	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED
EU	TRES SECRET UE / EU TOP SECRET	SECRET UE / EU SECRET	CONFIDENTIEL UE / EU CONFIDENTIAL	RESTREINT UE / EU RESTRICTED

Note 1: Diffusion Restreinte/Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects “ESA RESTRICTED” information in a manner no less stringent than the standards and procedures described in the ESA Security Regulations.

Note 2: France handles and protects Classified Information bearing the marking “ESA RESTRICTED” or equivalent according to its national laws and regulations in force for the protective level “DIFFUSION RESTREINTE” or the standards defined in the present document whichever is higher. ESA handles and protects information marked “DIFFUSION RESTREINTE” according to its Security Regulations and Directives as ESA RESTRICTED.

ANNEX 3

EUROPEAN SPACE AGENCY

COURIER CERTIFICATE

COURIER CERTIFICATE N°. .....
for the international hand-carriage of classified documents, equipment or components classified ESA CONFIDENTIAL or ESA SECRET.

This is to certify that the bearer:

Mr./Ms. .....(name/title)

Born on: .....(day/month/year) in..... (country)

A national of: .....(country)

Holder of passport/identity card N°.: .....(number)

Issued by: ..... (issuing authority)

On: .....(day/month/year)

Employed with: .....(company or organisation)

is authorised to carry on the journey detailed below the following consignment: (Number and particulars of the consignment in detail, i.e. number. of packages, weight and dimensions of each package and other identification data as in shipping documents)

.....

.....

.....

The attention of Customs, Police and/or Immigration Officials is drawn to the following :

- According to Annex 1, Article XIV, XVI, XVII of the Convention for the establishment of a European Space Agency entered into force on 30 October 1980, ESA staff members, experts and representatives of Member States enjoy privileges and immunities. In particular, they enjoy inviolability for all their official papers and documents.

- According to Article XII of Annex I of its Convention, for its official communications and the transfer of all its documents ESA enjoys treatment as favourable as other International Organisations. The material comprising this consignment is classified in the security interests of ESA and its Member States.

It is therefore requested that:

(a) the consignment will not be inspected without permission of a duly authorised representative of ESA nor retained ;

(b) It is requested that the consignment will not be inspected by other than properly authorised persons or those having special permission.

(c) If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not belong to the service and, in the presence of the courier.

(d) It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

(e) customs, policy and/or immigration officials of countries to be transited, entered or exited are requested to give assistance if necessary to ensure successful and secure delivery of the consignment.

The material comprising this consignment is classified in the interests of the security of:

.....

(Indicate the countries having interest. At least the country of origin of the shipment and that of the destination should be indicated. The country(-ies) to be transited may also be indicated).

(LETTERHEAD)

**Appendix to the "Courier Certificate" No.....
for the international hand-carriage of classified documents, equipment or components classified ESA CONFIDENTIAL or ESA SECRET.**

NOTES FOR THE COURIER

- You have been appointed to carry/escort a classified consignment. Your "COURIER CERTIFICATE" has been provided. Before starting the journey, you will be briefed on the security regulations governing the hand carriage of the classified consignments and on your security obligations during the specific journey (behaviour, itinerary, schedule, etc). You will also be requested to sign a declaration that you have read and understood and will comply with prescribed security obligations.

- The following general points are brought to your attention:

1. You will be held liable and responsible for the consignment described in the Courier Certificate;

2. Throughout the journey, the classified consignment must stay under your personal control;

3. The consignment will not be opened en route except in the circumstances described in sub-paragraph 10 below;

4. The classified consignment is not to be discussed or disclosed in any public place;

5. The classified consignment is not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance and storage facilities may be utilised. You are to be instructed on this matter by your company Security Officer;

6. While hand carrying a classified consignment, you are forbidden to deviate from the travel schedule provided;

7. In cases of emergency, you much take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal control; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as stated in the courier certificate above. If you have not received these details, ask for them from your company Security Officer';

8. You and the company Security Officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc) are complete, valid and current;

9. If unforeseen circumstances make it necessary to transfer the consignment to an individual other than the designated representatives of the company or government you are to visit, you will give it only to authorised employees of one of the points of contact listed in sub-paragraph 15 below;

10. There is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing; therefore, should such officials inquire into the contents of the consignment, show them your "Courier Certificate" and this note and insist on showing them to the senior Customs, Police and/or Immigration Official; this action should normally suffice to allow the consignment to pass through unopened. However, if the senior Customs, Police and/or Immigration Official demands to see the actual contents of the consignments you may open it in his presence, but this should be done in an area out of sight of the general public.

11. You should take precautions to show officials the minimum content necessary to them that the consignment does not contain any other item and ask the official to repack or assist in re-packing it immediately upon completion of the examination.

12. You should request the senior Customs, Police and/or Immigration Official to provide evidence of the opening and inspection of the packages by signing and sealing them when closed and confirming in the shipping documents (if any) that the consignment has been opened.

13. If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving company Security Officer and the dispatching company Security Officer, who should be requested to inform the DSA's of their respective governments.

14. Upon your return, you must produce a bona fide receipt for the consignment signed by the Security Officer of the company or agency receiving the consignment or by a DSA of the receiving government.

15. Along the route you may contact the following officials to request assistance:

.....

.....

From : ..... (originating country)

To : ..... (destination country)

Through : ..... (list intervening countries)

Authorised stops : ..... (list locations)

Date of beginning of journey: ..... (day/month/year)

Signature issuing Security Officer

Stamp

N O T E: (To be signed on completion of journey)

I declare in good faith that, during the journey covered by the "Courier Certificate", I am not aware of any occurrence or action, by myself or by others, which could have resulted in the compromise of the consignment.

Courier's Signature:

.....

Witnessed by:

.....
(Security Officer's signature)

Date of return of the "Courier Certificate":

.....
(Day/month/year)

ANNEX 4

EUROPEAN SPACE AGENCY

**MULTI-TRAVEL COURIER CERTIFICATE N° .....
for the international hand-carriage of classified documents, equipment or components classified ESA CONFIDENTIAL or ESA SECRET.**

This is to certify that the bearer Mr/Ms (name and title)

.....

born on: .....(day, month, year) in..... (country)

.....

a national of: ..... (country) .....

holder of passport or identity card N°:.....

issued by: .....(issuing authority) : .....

on: ..... (day, month, year)

employed by (company or organisation) :

.....

is authorized to carry classified documents, equipments and/or components between the following countries :

.....

.....

The bearer above is authorized to use this certificate as many times as necessary, for classified shipments between the countries here above until:

.....(date)

The shipment description should be attached to each consignment.

The attention of customs authorities, police and immigration services is drawn to the following points:

- The material forming each consignment is classified in the interest of national security of the countries here above.

- It is requested that the consignment will not be inspected by other than properly authorized persons or those having special permission.

- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not have a need-to-know and in the presence of the courier.

- It is requested that the package, if opened for inspection, be marked after re-closing to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

- Customs, Police and/or Immigration officials of countries to be transited, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.

Signature of the Security Officer

Signature of the Security Authority

(LETTERHEAD)

**Appendix to the "Courier Certificate" N°.....
for the international hand-carriage of classified documents, equipment or components classified ESA CONFIDENTIAL or ESA SECRET.**

NOTES FOR THE COURIER

You have been appointed to carry/escort classified consignments. Your "Courier certificate" has been provided. Before starting your journeys, you will be briefed on the security regulations governing the hand carriage of the classified consignments and on your obligations during the specific journey (behaviour, itinerary, schedule, etc). You will also be requested to sign a declaration that you have read and understood and will comply with prescribed security obligations.

The following general points are brought to your attention:

1. You will be held liable and responsible for the consignments described in the "descriptions of shipments".
2. Throughout the journey, the classified consignments must stay in your personal possession, unless you are accompanying a classified consignment under NSA/DSA approved transportation plan.
3. The consignments will not be opened en route except in the circumstances described in paragraph 10 below.
4. The classified consignments are not to be discussed or disclosed in any public place.
5. The classified consignments are not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance may be utilized. You are to be instructed on this matter by your company security officer.
6. While hand carrying or accompanying a classified consignment, you are forbidden to deviate from the schedule provided.
7. In case of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal possession except under circumstances described in paragraph 2 above; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as stated in the multi-travels courier certificate above. If you have not received these details, ask for them from your company security officer.

8. You and the company security officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc) are complete, valid and current.
9. If unforeseen circumstances make it necessary to transfer a consignment to other than the designated representative of the company or government you are to visit, you will give it only to authorized employees of one of the points of contact listed in the description of shipment.
10. There is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing; therefore, should such officials enquire into the contents of the consignment, show them your "courier certificate" the description of shipment and this note and insist on showing them to the senior Customs, Police, and/or Immigration Official; This action should normally suffice to allow the consignment to pass through unopened. However, if the senior Customs, Police, and/or Immigration Official requests to see the actual contents of the consignment you may open it in his presence, but this should be done in area out of sight of the general public.
11. You should take precautions to show officials only as much of the contents as will satisfy them that the consignment does not contain any other item and ask the official to repack or assist in repacking it immediately upon completion of the examination.
12. You should request the senior Customs, Police, and/or Immigration Official to provide evidence of the opening and inspection of the consignment by signing and sealing them when closed and confirming in the shipping documents (if any) that the consignment has been opened.
13. If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving company Security Officer and the dispatching company Security Officer, who should be requested to inform the NSA/DSA of their respective governments.
14. Along the route you may contact the officials whose details will be provided to you before each journey and request assistance from them.
15. Upon return from each journey, you must produce a bona fide receipt for the consignment signed by the Security Officer of the company or agency receiving the consignment or by a NSA/DSA of the receiving government.

To multi-travels courier certificate No:.....

Description of shipment No : .....

Transport from:.....(date) to .....(date)

Bearer (name) : .....

Itinerary : from:..... (originating country)

to: ..... (destination country)

Through:..... (crossed countries)

Authorized stops: ..... (list of locations)

References of receipt or inventory list : .....

Description of the shipment (number of package, dimensions and, if needed, the weight of each package) :

.....

.....

Officials you may contact to request assistance:

.....

.....

Signature of company's Security Officer

Note to be signed on completion of each shipment:

I declare in good faith that, during the journey covered by this "shipment description", I am not aware of any occurrence or action, by myself or by other, that could have resulted in the compromise of the consignment, except the events related below, if needed :

Place and date of declaration : .....

Courier's signature : .....

Witnessed by (name and signature of company Security Officer):

.....

ANNEX 5

Facility Security Clearance Information Sheet (FIS)

REQUEST

Please [ ] provide a FSC assurance of the facility listed below

[ ] start initiating a FSC up to and including the level of... if the facility does not hold a current FSC

[ ] confirm the FSC up to and including the level of ... .

provided on ..... (dd/mm/yy)

[ ] provide the correct and complete information, if applicable.

	corrections/completions:
1. Full facility name:	
_____	_____
2. Full facility address:	
_____	_____
3. Mailing address (if different from 2):	
_____	_____
4. Zip code/city/country:	
_____	_____
5. Name/phone/fax/e-mail of the security officer:	
_____	_____

6. This request is made for the following reason(s):
(indicate particulars of the pre-contractual stage, contract, sub-contract, programme/project)

_____

_____

_____

REQUESTING AUTHORITY:

Name:..... **Date:.....**

REPLY

1. This is to inform you that the above mentioned facility:

[ ] holds a FSC up to and including the level of [ ] S [ ] C

[ ] does not hold a FSC

[ ] does not hold a FSC but, on your above mentioned request, the FSC is in progress. You will be informed when the FSC has been established.

Expected date: ...../..... (mm/yy) [if known]

2. Safeguarding of classified documents: [ ] yes, level: ..... [ ] no

Safeguarding of classified material : [ ] yes, level: ..... [ ] no

3. This FSC certification expires on:.....(dd/mm/yy).

You will be informed in case of an earlier invalidation or significant change to any information listed above.

4. Should any contract be let or Classified Information be transferred in relation to this certification, please inform us on all relevant data including security classification.

5. REMARKS:

.....

.....

.....

PROVIDING AUTHORITY:

Name:..... Date:.....

ANNEX 6

REQUEST FOR VISIT

☐ Single Visit

☐ Recurring Visit

1. ADMINISTRATIVE DATA

Requestor: .....

Date request: .....

Visit ID: .....

Sent to: .....

2. REQUESTING GOVERNMENT AGENCY/INDUSTRIAL FACILITY / INTERNATIONAL ORGANISATION

Name: .....

Point of contact: .....

Postal address: .....

.....

Telephone nr: ..... Telefax nr: .....

Email address: .....

3. GOVERNMENT AGENCY/INDUSTRIAL FACILITY / INTERNATIONAL ORGANISATION TO BE VISITED

Name: .....

Point of contact: .....

Postal address: .....

.....

Telephone nr: ..... Telefax nr: .....

Email address: .....

4. DATES OF VISIT

From ..... / ..... / ..... to ..... / ..... / .....

5. TYPE OF VISIT

Government initiative ☐ Commercial initiative ☐

By invitation of facility to be visited ☐ Initiated by requesting agency/facility ☐

6. SUBJECT TO BE DISCUSSED

.....

.....

7. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION INVOLVED

.....

8. PARTICULARS FOR VISITORS

Company/Agency/Int.Org: ....

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

- Name: .... First name: ....

  Place of birth: ....Date of birth: ....

  Nationality: .... ID/PP Nr: ....

  In possession of a valid security clearance for the indicated level: YES ☐ NO ☐

9. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY/ INDUSTRIAL FACILITY/INTERNATIONAL ORGANISATION

Name: ..... First name: .....

Telephone nr: ..... Fax nr: .....

Email address: .....

10. CERTIFICATION OF SECURITY CLEARANCE

Name: ..... First name: .....

Telephone nr: ..... Fax nr: .....

Email address: .....

STAMP

11. REQUESTING SECURITY AUTHORITY

Name: ..... First name: .....

Telephone nr: ..... Fax nr: .....

Email address: .....

STAMP

12. HOSTING SECURITY AUTHORITY

Name: ..... First name: .....

Telephone nr: ..... Fax nr: .....

Email address:
.....

STAMP

13. REMARKS