Vorblatt

Problem:

Österreichische Wissenschafter und Unternehmen erhalten nur unter der Voraussetzung gleichberechtigten Zugang zu wichtigen Ausschreibungen und Aufträgen der ESA, insbesondere für Galileo, das weltweite unabhängige europäische Radionavigationssystem, wenn Österreich Vertragspartei des ESA-Sicherheitsübereinkommens wird.

Ziel:

Gleichberechtigter Zugang österreichischer Wissenschafter und Unternehmen zu allen Ausschreibungen und Aufträgen der ESA.

Inhalt:

Regelung des Schutzes und der Sicherung der im Rahmen der ESA verwendeten geheimhaltungsbedürftigen Informationen.

Alternativen:

Keine.

Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Förderung der österreichischen Weltraumindustrie, in der ca. 300 Personen beschäftigt sind.

Finanzielle Auswirkungen:

Die durch zusätzliche Überprüfungsmaßnahmen verursachten Kosten werden durch die interessierten Unternehmen zu tragen sein (vgl. § 55b Abs. 5 SPG).

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Im Bereich der EU bestehen ebenfalls Regelungen über den Schutzes und der Sicherung klassifizierter Informationen, deren Einhaltung in Österreich durch das Informationssicherheitsgesetz (InfoSiG) sichergestellt wird.

Besonderheiten des Normerzeugungsverfahrens:

Beschluss des Nationalrats gemäß Art. 50 Abs. 2;

Sonderkundmachung der französischen Sprachfassung des Übereinkommens gemäß Art. 49 Abs. 2 B-VG.

Erläuterungen

Allgemeiner Teil

Das Übereinkommen zwischen den Vertragsstaaten des Übereinkommens zur Gründung einer Europäischen Weltraumorganisation und der Europäischen Weltraumorganisation über den Schutz und den Austausch geheimhaltungsbedürftiger Informationen ist gesetzändernd und gesetzesergänzend und bedarf daher der Genehmigung durch den Nationalrat gemäß Art. 50 Abs. 1 B-VG. Es hat nicht politischen Charakter und enthält keine verfassungsändernden bzw. verfassungsergänzenden Bestimmungen. Das Übereinkommen ist der unmittelbaren Anwendung im innerstaatlichen Rechtsbereich nicht zugänglich, sodass eine Erlassung von Gesetzen gemäß Art. 50 Abs. 2 B-VG erforderlich ist. Einer Zustimmung des Bundesrates gemäß Art. 50 Abs. 1 zweiter Satz B-VG bedarf es nicht, da keine Angelegenheiten des selbständigen Wirkungsbereiches der Länder geregelt werden.

Österreich ist Mitglied der Europäischen Weltraumorganisation (ESA), vgl. das Übereinkommen zur Gründung einer Europäischen Weltraumorganisation, BGBl. Nr. 95/1987 (ESA-Übereinkommen). Im Rahmen der ESA wurde ein Übereinkommen über den Schutz und den Austausch geheimhaltungsbedürftiger Informationen („ESA-Sicherheitsübereinkommen“) ausgearbeitet, das der ESA-Rat in seiner Sitzung am 13. Juni 2002 genehmigt hat. Mit diesem Übereinkommen sollte ein geeignetes Rechtsinstrument geschaffen werden, um ein angemessenes Schutzniveau für geheimhaltungsbedürftige Informationen innerhalb der ESA und in ihren Mitgliedstaaten zu gewährleisten (vgl. 4. Präambularabsatz des Übereinkommens).

Zentrale Bestimmung des ESA-Sicherheitsübereinkommens ist dessen Art. 2, demzufolge die Vertragsparteien bestimmte, als solche gekennzeichnete geheimhaltungsbedürftige Informationen „entsprechend den vereinbarten Geheimschutzgrundsätzen und Mindestnormen“ schützen und sichern werden. Bei diesen Grundsätzen und Normen handelt es sich um die ESA-Sicherheitsbestimmungen, die vom ESA-Rat am 11. Dezember 2002 (Teil I) und am 12. Juni 2003 (Teil II) gemäß Art. XI Abs. 5 lit. m und Abs. 6 lit. d ESA-Übereinkommen mit einfacher Mehrheit beschlossen wurden. Durch Art. 2 und 3 des ESA-Sicherheitsübereinkommens werden die ESA-Sicherheitsbestimmungen mittelbarer Vertragsbestandteil des ESA-Sicherheitsübereinkommens; sie werden daher den Erläuterungen als Anlage beigeschlossen und aus Gründen der Publizität gemäß § 2 Abs. 5 Z 5 BGBlG im Teil III des Bundesgesetzblattes zu verlautbaren sein.

Das ESA-Sicherheitsübereinkommen wurde bereits von sieben Staaten unterzeichnet (Belgien, Deutschland, Finnland, Frankreich, Italien, Portugal und Schweden) und von zwei dieser Staaten (Italien, Schweden) auch schon ratifiziert. Gemäß seinem Art. 10 Abs. 2 ist das Übereinkommen nach Hinterlegung der zweiten Ratifikations-, Annahme oder Genehmigungsurkunde am 20. Juni 2003 für die betreffenden Staaten in Kraft getreten.

Eine rasche Unterzeichnung und Ratifikation des ESA-Sicherheitsübereinkommens durch Österreich ist insbesondere notwendig, um österreichischen Wissenschaftlern und Unternehmen den gleichberechtigten Zugang zu Ausschreibungen und Aufträgen der ESA für Galileo, dem weltweiten unabhängigen europäischen Radionavigationssystem, zu ermöglichen. Die Ausschreibung für die fliegenden Teile (IOV – In Orbit Validation – Phase) wird bereits im November 2003 erfolgen.

Die innerstaatliche Umsetzung des ESA-Sicherheitsübereinkommens kann nur teilweise im Rahmen bestehender gesetzlicher Regelungen erfolgen; es werden daher bis zur Ratifikation des ESA-Sicherheitsübereinkommens ergänzende gesetzliche Regelungen vorzunehmen sein.

Das ESA-Sicherheitsübereinkommen kann nicht als Regierungsübereinkommen geschlossen werden, da es Bestimmungen enthält, die von der in § 5 Abs. 2 des Bundesgesetzes über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz - InfoSiG), BGBl. I Nr. 23/2002, enthaltenen gesetzlichen Grundlage für den Abschluss von Regierungsübereinkommen über die Übermittlung klassifizierter Informationen nicht erfasst sind.

Besonderer Teil

Zu Art. 1:

Art. 1 definiert den Begriff „geheimhaltungsbedürftige Informationen“ nach der Möglichkeit einer Schädigung der Interessen der Vertragsparteien und der Kennzeichnung der Informationen („Geheimhaltungsgrad“). Die ESA-Sicherheitsbestimmungen (zu diesen sh. Allgemeiner Teil) sehen in Teil I Z 5 die (hier

auf die ESA bezogenen) international üblichen Klassifizierungsstufen ESA TOP SECRET (ESA TS) – streng geheim, ESA SECRET (ESA S) – geheim, ESA CONFIDENTIAL (ESA C) – vertraulich und ESA RESTRICTED (ESA R) – eingeschränkt vor. Zu den Klassifizierungsstufen vgl. auch § 2 Abs. 2 InfoSiG.

Zu Art. 2:

Z 1 definiert den Begriff „geheimhaltungsbedürftige Informationen“ nach deren Herkunft oder Verwendung: Informationen sind zu schützen und zu sichern, die von der ESA herausgegeben, der ESA von einem ESA-Mitgliedstaat zur Verfügung gestellt (Z 1 lit. a) oder die von einem ESA-Mitgliedstaat einem anderen zur Unterstützung einer ESA-Aktivität zur Verfügung gestellt werden (Z 1 lit. b). Z 2 bis 4 betreffen die Beibehaltung des Schutzniveaus, die zweckbestimmte Verwendung und die Zustimmung des Herausgebers einer Information als Voraussetzung für deren Weitergabe.

Ein ergänzender gesetzlicher Regelungsbedarf zur Umsetzung des ESA-Sicherheitsübereinkommens in Österreich (vgl. dazu auch Allgemeiner Teil) ergibt sich insbesondere im Hinblick auf die in den ESA-Sicherheitsbestimmungen (Teil I Z 46 ff.) angesprochene industrielle Sicherheit. So bestimmt Z 46, dass alle Einrichtungen, die an wirtschaftlichen Aktivitäten teilnehmen, die mit einem Zugang zu als ESA CONFIDENTIAL oder darüber klassifizierten Informationen verbunden sind, über eine „Facility Security Clearance“ verfügen müssen. Für die Ausstellung solcher Bescheinigungen ist in der österreichischen Rechtsordnung noch eine Grundlage zu schaffen.

Zu Art. 3:

Art. 3 ist eine Auslegungsnorm, die auf ein gemeinsames Schutzniveau für geheimhaltungsbedürftige Informationen abzielt.

Zu Art. 4:

Abs. 1 sieht Sicherheitsüberprüfungen für Personen vor, die in Ausübung ihrer amtlichen Tätigkeit („conduct of their official duties“) Zugang zu geheimhaltungsbedürftigen Informationen benötigen. Sicherheitsüberprüfungen sind in Österreich in den §§ 55 bis 55b des Bundesgesetzes über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG), BGBl. Nr. 566/1991 idgF, vorgesehen, vgl. aber auch die Verlässlichkeitsprüfungen gemäß den §§ 23 und 24 des Bundesgesetzes über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz - MBG), BGBl. I Nr. 86/2000 idgF.

Abs. 2 bestimmt, dass nur solchen Personen Zugang zu geheimhaltungsbedürftigen Informationen gegeben werden darf, die zur Erfüllung ihrer Aufgaben oder Aufträge (von diesen Informationen) Kenntnis haben müssen. Dieses „need to know“-Prinzip kommt auch in § 3 Abs. 1 Z 1 lit. a und Z 2 lit. a InfoSiG zum Ausdruck.

Die in Abs. 4 und Art. 6 Abs. 2 vorgesehene internationale Zusammenarbeit findet im Wege der gemäß den ESA-Sicherheitsbestimmungen (Teil I Z 2) vorzusehenden „National Security Authority“ statt. Es ist beabsichtigt, die durch § 8 InfoSiG errichtete Informationssicherheitskommission auch für die Zwecke des ESA-Sicherheitsübereinkommens als „National Security Authority“ zu notifizieren.

Zu Art. 5:

Art. 5 betrifft die Anwendung des Übereinkommens innerhalb der ESA.

Zu Art. 6:

Abs. 1 verpflichtet die Vertragsparteien, Fälle der Preisgabe und des Verlustes von geheimhaltungsbedürftigen Informationen zu untersuchen. Innerstaatlich trifft diese Verpflichtung – unvorgreiflich einer weiteren gesetzlichen Regelung – primär den Informationssicherheitsbeauftragten des sachlich zuständigen Bundesministeriums (§ 7 InfoSiG).

Zu Art. 7:

Art. 7 verpflichtet die ESA-Mitgliedstaaten, den ESA-Rat und den ESA-Generaldirektor im Einklang mit verschiedenen Bestimmungen des ESA-Übereinkommens, BGBl. Nr. 95/1987, zur Aufhebung der Immunität, wenn es sich um Gerichtsverfahren über die unbefugte Preisgabe geheimhaltungsbedürftiger Informationen handelt.

Zu Art. 8:

Art. 8 stellt klar, dass das Übereinkommen die Vertragsparteien nicht daran hindert, andere, den Anwendungsbereich des Übereinkommens nicht berührende Übereinkünfte über den Austausch von geheimhaltungsbedürftigen Informationen, deren Herausgeber sie sind, zu schließen

Zu Art. 9 bis 13:

Diese Artikel enthalten die üblichen Schlussklauseln und betreffen Änderungen des Übereinkommens (Art. 9), dessen Unterzeichnung und Inkrafttreten (Art. 10), Beitritte (Art. 11), die Kündigung (Art. 12) und die Aufgaben des Depositärs (Frankreich, Art. 13).

ANLAGEN

Anlage 1: ESA Security Regulations – Part I and II, englische Sprachfassung

Anlage 2: Sicherheitsvorschriften der ESA – Teil I und II, Übersetzung ins Deutsche

Anlage 1 Teil I der Erläuterungen

ESA SECURITY REGULATIONS PART I

BASIC PRINCIPLES AND MINIMUM STANDARDS FOR THE PROTECTION OF CLASSIFIED INFORMATION PRODUCED AND TRANSMITTED IN CONNECTION WITH ESA ACTIVITIES

INTRODUCTION

1. These provisions lay down the basic principles and minimum standards of security to be applied by the European Space Agency (hereinafter called "ESA") and by the Member States so that ESA classified information is safeguarded from loss of confidentiality, integrity and availability. Security programmes shall be established to meet these basic principles and standards throughout ESA and its Member States to ensure a common degree of protection in accordance with article 3 of the ESA Security Agreement.
2. ESA Security has the following principal objectives:
   (a) to safeguard ESA classified information from espionage, compromise or unauthorised disclosure;
   (b) to safeguard ESA classified information handled in communications and information systems and networks, against threats to its integrity and availability;
   (c) to safeguard installations housing ESA classified information from sabotage and malicious wilful damage;
   (d) in the event of failure, to assess the damage caused, limit its consequences and adopt the necessary remedial measures.
3. The foundations of sound security are:
   (a) within each Member State, a National Security Authority (NSA)/Designated Security Authority (DSA) which is responsible for ensuring that a security determination of eligibility has been made in respect of all nationals who are required to have access to information classified ESA CONFIDENTIAL and above.
   (b) within each Member State, a national security structure responsible for:
      (i) the collection and recording of intelligence on espionage, sabotage, terrorism and other subversive activities, and
      (ii) information and advice to its government, and through it, to the ESA Council, on the nature of the threats to security and the means of protection against them;
   (c) within each Member State, and within ESA, a technical INFOSEC authority responsible for working with the security authority concerned to provide information and advice on technical threats to security and the means for protection against them;
   (d) regular collaboration among government departments, agencies and the appropriate ESA services, in order to establish, and recommend, as appropriate:
      (i) what information, resources and installations need to be protected, and
      (ii) common standards of protection.
4. Where confidentiality is concerned, care and experience are needed in the selection of information and material to be protected and the assessment of the degree of protection it requires. It is fundamental that the degree of protection corresponds with the security classification of the individual piece of information and material to be protected. In order to ensure the smooth flow of information, steps shall be taken in order to avoid over classification. The classification system is the instrument for giving effect to these principles**.** The same system of classification should be followed in planning and organising ways to counter espionage, sabotage, terrorism and other threats so that the greatest measure of protection is given to the most important premises housing ESA classified information and to the most sensitive points within them.

Classification management

5. Levels of classification

Information is classified at the following levels:

ESA TOP SECRET (ESA TS): 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.

ESA SECRET (ESA S): 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.

ESA CONFIDENTIAL (ESA C): 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.

ESA RESTRICTED (ESA R): 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.

6. Information shall be classified only when necessary. The classification shall be clearly and correctly indicated, and shall be maintained only as long as the information requires protection.
7. The responsibility for classifying information rests solely with the originator. ESA classified documents may be downgraded or declassified only with the prior written consent of the originator and, if necessary, after discussion with other interested parties.

BASIC PRINCIPLES

8. The security measures shall:
   (a) extend to all persons having access to ESA classified information, classified information-carrying media, all premises containing such information and important installations;
   (b) be designed to detect persons whose position might endanger the security of classified information and important installations housing ESA classified information and provide for their exclusion or removal;
   (c) prevent any unauthorised person from having access to ESA classified information or to installations which contain it;
   (d) ensure that ESA classified information is disseminated solely on the basis of the need-to-know principle which is fundamental to all aspects of security;
   (e) ensure the integrity (i.e. prevention of corruption or unauthorised alteration or unauthorised deletion) and the availability (i.e. access is not denied to those needing and authorised to have access) of all ESA classified information, and especially of such information stored, processed or transmitted in electromagnetic form.

ORGANISATION OF SECURITY

9. The ESA Director General and each Member State shall ensure that common minimum standards of security are observed by all national bodies, by ESA headquarters, establishments and facilities, and by contractors so that ESA classified information can be passed in the confidence that it will be handled with equal care. Such minimum standards shall include criteria for the clearance of personnel, and procedures for the protection of ESA classified information.
10. In particular, for ESA the Director General shall:
    (a) implement the ESA Security Regulations;
    (b) consider security problems referred to him by the ESA Headquarters, establishments and facilities;
    (c) examine questions involving changes in the ESA Security Regulations, in close liaison with the NSA/DSA or any national competent authority of the Member States.
11. A Security Committee is set up by the ESA Council. It should include delegates of the Member States also representing the appropriate national security authorities. It is chaired by a chairman and a vice-chairman elected from Member States representatives. The Security Committee advises the ESA Council on all issues of security within the framework of its terms of reference.
12. In order to fulfil the above-mentioned responsibilities, the ESA Director General shall have the ESA Security Office at his disposal. The Head of the ESA Security Office shall be responsible for coordinating, supervising and implementing security measures including security of IT systems and networks.
13. In each Member State a NSA/DSA responsible for the security of ESA classified information should be designated. This NSA/DSA should, in particular 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 an ESA TOP SECRET central registry;

(c) the periodic inspection of the security arrangements for the protection of ESA classified information;

(d) ensuring that all persons employed within national bodies who in the conduct of their official duties require access or whose duties or function may afford access to ESA information classified ESA TOP SECRET, ESA SECRET and ESA CONFIDENTIAL are appropriately security cleared before they are granted access to such information**.**

(e) devising such security plans as are considered necessary to prevent ESA classified information from falling into the hands of unauthorised persons.

14. Periodic inspections of the security arrangements for the protection of ESA classified information in ESA shall be carried out by the ESA Security Office and by the NSA/DSA concerned, jointly and in mutual agreement.

SECURITY OF PERSONNEL

Clearance of personnel

15. Access to ESA classified information will be authorised only for persons having a "need-to-know" for carrying out their duties or missions. The responsibility for determining the "need-to-know" will rest with the ESA Director General, the Head of ESA headquarters, establishments or facilities and with the national body in which the person concerned is to be employed, according to the requirements of the task.

16. All persons who in the conduct of their official duties require access or whose duties or functions may afford access to information classified ESA CONFIDENTIAL or above, shall be appropriately security cleared before they are granted access to such information. Similar clearance shall be required in the case of persons whose duties involve the technical operation or maintenance of communication and information systems containing classified information.

This clearance shall be designed to determine in particular whether such individuals:

(a) are of unquestioned loyalty;

(b) are of such character and discretion as to cast no doubt upon their integrity in the handling of ESA classified information; or

(c) may be vulnerable to pressure from foreign or other sources, e.g. due to former residence or past associations which might constitute a risk to security.

17. Particularly close scrutiny in the clearance procedures shall be given to persons:

(a) to be granted access to ESA TOP SECRET information;

(b) occupying positions involving regular access to a considerable volume of ESA SECRET information;

(c) whose duties give them special access to mission-critical communication or information systems and thus the opportunity to gain unauthorised access to large amounts of ESA classified information or to inflict serious damage upon the mission through acts of technical sabotage.

In the circumstances outlined in subparagraphs (a), (b) and (c), the fullest practicable use shall be made of the technique of background investigation.

18. The security clearance procedure shall be carried out at the request of the appointing authority by the NSA/DSA or any national competent authorities of the Member State of which the person is a national. Should the person concerned reside in the territory of another Member State, the national authorities concerned may secure the cooperation of the authorities of the State of residence. When the person is not a national of a Member State, it is the responsibility of the NSA/DSA or national competent authority of the Member State where this person works and/or resides to carry out the security clearance procedure.

19. The appointing authority shall specify in its request the type and level of ESA classified information to be made available to the person concerned, so that the NSA/DSA or national competent authorities can carry out the security clearance procedure and give their opinion as to the level of clearance it would be appropriate to grant to that person.

20. The whole security clearance procedure together with the results obtained shall be subject to the relevant rules and regulations in force in the Member State concerned, including those concerning appeals.

21. Exceptionally, pending the outcome of the security clearance procedure, the ESA Director General may, with the agreement of the NSA/DSA or national competent authority, grant

temporary access authorisation for information classified up to and including ESA SECRET only, for a period not exceeding six months, to an ESA staff member.

Records of personnel security clearances

22. National bodies, ESA headquarters, establishments and facilities, or contractors handling ESA classified information or housing mission-critical communication or information systems shall maintain a record of the clearances granted to the persons assigned thereto. Each clearance shall be verified as the occasion demands to ensure that it is adequate for that person's current assignment; it shall be re-examined as a matter of priority whenever new information is received indicating that continued assignment on classified work is no longer consistent with the interests of security. The record of clearances shall be held by the head of security for the national body, ESA headquarters, establishment and facility, or contractor concerned.

Security instruction of personnel

23. All persons employed in positions where they could have access to classified information shall be thoroughly instructed on taking up assignment and at regular intervals in the need for security and the procedures for accomplishing it. All such persons should certify in writing that they fully understand the security regulations relevant to their assignment.

Management responsibilities

24. Managers shall have the duty of knowing those of their staff who are engaged in classified work or who have access to mission-critical communication or information systems and of recording and reporting any incidents or apparent vulnerabilities, likely to have a bearing on security.

Security status of personnel

25. Procedures shall be established to ensure that, when adverse information becomes known concerning a person, it is determined whether the person is employed on classified work or has access to mission-critical communication or information systems, and the authority concerned informed. If it is established that such a person constitutes a security risk, he or she shall be barred or removed from assignments where he or she might endanger security.

ESA TOP SECRET REGISTRIES

26. The purpose of ESA TOP SECRET registries is to ensure the recording, handling and distribution of ESA TOP SECRET documents in accordance with the ESA Security Regulations.
27. Central registries will act as the main receiving and despatching authority in Member States and in the ESA Headquarters, in which such registries have been set up.

BREACHES OF SECURITY AND COMPROMISE OF ESA CLASSIFIED INFORMATION

28. A breach of security occurs as the result of an act or omission contrary to an ESA or national security regulation, which might endanger or compromise ESA classified information.
29. Compromise of ESA classified information occurs when it has wholly or in part fallen into the hands of unauthorised persons, i.e. 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.
30. ESA classified information may be compromised as a result of carelessness, negligence or indiscretion as well as by the activities of services which target ESA or its Member States, as regards ESA classified information and activities, or by subversive organisations.
31. It shall be the duty of each security authority, as soon as it is notified that such a breach of security may have occurred, to report the fact immediately to the ESA Security Office.
32. Any individual who is responsible for compromising ESA classified information shall be liable to disciplinary action according to the relevant rules and regulations. Such action shall be without prejudice to any other legal action. ESA staff members shall be informed about the possible legal consequences of breaches of security and in particular about Article 7 of the ESA Security Agreement on the possible waiver of immunity.

PHYSICAL SECURITY

Need for protection

33. The degree of physical security measures to be applied to ensure the protection of ESA classified information shall be proportional to the classification, volume of and threat to the information and material held. Therefore care shall be taken to avoid both over- and under-classification, and classification shall be subject to regular review. All holders of ESA classified information shall follow uniform practices regarding classification of that information and meet common standards

of protection regarding custody, transmission and disposal of information and material requiring protection.

Checking

34. Before leaving areas containing ESA classified information unattended, persons having custody thereof shall ensure that it is securely stored and that all security devices have been activated (locks, alarms, etc.). Further independent checks shall be carried out after working hours.

Security of buildings

35. Buildings housing ESA classified information or mission-critical communication and information systems shall be protected against unauthorised access. The nature of the protection afforded to ESA classified information, e.g. barring of windows, locks for doors, guards at entrances, automated access control systems, security checks and patrols, alarm systems, intrusion detection systems and guard dogs, shall depend on:
    (a) the classification, volume and location within the building of the information and material to be protected;
    (b) the quality of the security containers for this information and material;
    (c) the physical nature and location of the building.
36. The nature of the protection afforded to communication and information systems shall similarly depend upon an assessment of the value of the assets at stake and of the potential damage if security were compromised, upon the physical nature and location of the building in which the system is housed, and upon the location of the system within the building.

Contingency plans

37. Detailed plans shall be prepared in advance for the protection of ESA classified information during a local or national emergency.

INFORMATION SECURITY (INFOSEC)

System Security Principles and Procedures

38. All communications, information systems and networks (hereinafter SYSTEMS) handling ESA classified information require security measures to protect the confidentiality, integrity and availability of that information. The security measures to be applied to those systems will be determined by the appropriate Security Accreditation Authority (SAA) and will be commensurate with the assessed risk and consistent with the policy stated in the ESA Security Regulations.
39. 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.
40. All SYSTEMS handling information classified ESA CONFIDENTIAL and above shall be accredited.
41. There shall be a Security Accreditation Authority (SAA) responsible for ensuring the compliance of SYSTEMS with the ESA Security Regulations.
42. For SYSTEMS belonging to ESA, the SAA shall be:

- for a SYSTEM used by ESA headquarters, establishments and facilities:

- if the SYSTEM is not connected with a national information system and does not use or process national classified information, the accreditation process is an internal process;

- otherwise, a panel staffed by ESA and the appropriate NSA/DSA (of Member States concerned by interconnection or national classification) conducts the accreditation process and validates accreditation statements.

- for SYSTEMS used by national bodies or contractors, the NSA/DSA of the Member State where the SYSTEM is deployed. In such a case the NSA/DSA conducts the accreditation process and validates accreditation statements.

43. For all SYSTEMS handling information classified ESA CONFIDENTIAL and above, a SYSTEM-Specific Security Requirement Statement (SSRS) shall be approved by the SAA.
44. Users of the SYSTEM shall be cleared and have a need-to-know, as appropriate for the classification and content of the information handled within their particular SYSTEM. Access to certain equipment (e.g. cryptographic) or information specific to security of SYSTEMS will require a special clearance issued by the relevant NSA/DSA.

COUNTER-SABOTAGE AND OTHER FORMS OF MALICIOUS WILFUL DAMAGE

45. Physical precautions for the protection of important installations housing classified information are the best protective security safeguards against sabotage and malicious wilful damage, and clearance of personnel alone is not an effective substitute.

INDUSTRIAL SECURITY

46. All entities participating in industrial activities, which involve access to information classified ESA CONFIDENTIAL and above must hold a Facility Security Clearance (FSC).
47. In respect of all contracts classified ESA CONFIDENTIAL and above, the prime contractor shall notify the NSA/DSA of the nation in which the entity that has been awarded the contract is located or incorporated, that a Security Aspect Letter (SAL) has been provided to that entity together with the contract.
48. The prime contractor shall be contractually required, under penalty of termination of their contract, to take all measures prescribed by ESA and/or NSAs/DSAs respectively for safeguarding all ESA classified information generated by or entrusted to the contractor, or embodied in articles manufactured by the contractor.
49. The prime contract shall contain a Programme Security Instruction (PSI) as an annex. A "Programme Security Classification Guide" shall be a part of the PSI. All other ESA classified contracts shall include, as a minimum, a "Security Aspect Letter" (SAL). In the latter case, the Programme/Project Security Classification Guide may be referred to as a "Security Classification Checklist". The PSI and/or SAL shall be the single source document for the security of the contract.
50. The prime contractor may negotiate subcontracts with other contractors, i.e., subcontractors. These subcontractors may also negotiate subcontracts with other subcontractors. The prime contractor will be responsible for all subcontracting activities.
51. All contractors, shall, for contracts classified ESA CONFIDENTIAL and above, always hold an FSC and shall ensure that their representatives involved in the negotiations hold appropriate PSC and only receive access to ESA classified information needed for the negotiation of the contract. For contracts classified ESA RESTRICTED, a FSC is not required unless specifically required by national security rules and regulations.
52. Applications for the security clearance for personnel of contractor facilities shall be made to the NSA/DSA, which is responsible for the facility. In submitting the request for verification or initiation of a PSC, the facility shall include:
    (a) the identity and security classification of the contract or subcontract, and
    (b) the level of ESA classified information to which the person concerned will have access.
53. If an entity wishes to employ a national of a non-ESA Member State in a position that requires access to ESA classified information, it is the responsibility of the NSA/DSA of the Member State in which the hiring facility is located and incorporated, to carry out the security clearance procedure prescribed herein, and determine that the person can be granted access in accordance with the provisions of the ESA Security Regulations, in particular paragraph 8 of Part I.

EXCHANGE OF CLASSIFIED INFORMATION BETWEEN ESA AND THIRD STATES OR INTERNATIONAL ORGANISATIONS

54. The exchange of ESA classified information with third States, international organisations or with other third parties shall be decided by the ESA Council.
55. Once the ESA Council has decided that there is a permanent or long-term or occasional need for the exchange of classified information between ESA and third States or other international organisations, the ESA Director General shall negotiate agreements on security procedures for the exchange of classified information or memoranda of understanding with them, defining the purpose of cooperation and the reciprocal rules on the protection of the information exchanged.
56. Draft agreements on security procedures or memoranda of understanding will be approved by the Security Committee before they are presented to the ESA Council for a decision.
57. The implementation of the release procedures of ESA classified information originating in ESA to a third State or an international organisation, shall rest with the Director General. If the originator of the information for which release is desired is not ESA, the Director General shall first seek the originator's prior written consent to release it. If the originator cannot be established, the appropriate ESA Board or Committee will assume the former's responsibility.

ANNEX

58. A comparative table of ESA and Member States' security gradings may be found in the Annex.

GLOSSARY OF TERMS

Accreditation: means the process, which confirms that a system will operate under the security conditions specified in the SYSTEM-Specific Security Requirement Statement (SSRS) or other relevant document and does not present an unacceptable risk.

Appointing authority: means the authority, which is competent to appoint a person and to request the security clearance.

Availability: means that the information and material is accessible and usable upon demand by an authorised individual or entity.

Competent authority: means an authority identified by the NSA of a Member State which is authorised to carry out personnel security clearances in order to give their nationals access to ESA classified information.

Contractor: means a legal person or body that agrees to supply goods or services whether as prime or single contractor or as subcontractor.

Designated Security Authority: 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.

Entity: means any legal person or body.

ESA classified information: means any information, document or material in whatever form whose unauthorised disclosure could damage the interests of one or more of the Parties to the ESA Security Agreement and which has been so designated by a security classification whether this information is originated by ESA or is submitted to ESA by a Member State or is submitted by a Member State to another Member State in support of an ESA programme, project or contract.

ESA Personnel Security Clearance: means a determination that an individual is eligible to have access to ESA classified information.

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 communication, information an other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of systems themselves.

Notes.

1. INFOSEC measures include those of computer transmission, emission and cryptographic security.
2. Such measures also include detection, documentation and countering of threats to information and to the systems.

Member State: refers to a State which is Party to the Convention of the European Space Agency in accordance with Articles XX and XXII of the said Convention.

National body: means any administrative and/or government department, office, service, agency or establishment of a Member State.

National Security Authority: means an authority of a Member State, which is responsible for the maintenance of security of ESA classified information in national bodies at home or abroad.

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

Programme Security Classification Guide: means part of the programme security instruction (PSI), which identifies the elements of the programme that are classified, specifying the security classification levels. The security classification guide may be expanded throughout the programme life cycle, and the elements of information may be re-classified or downgraded.

Programme Security Instruction: means a compilation of security regulations/procedures, which are applied to a specified programme in order to standardise security procedures. The PSI also constitutes an Annex to the main contract, and may be revised throughout the programme lifecycle. For sub-contracts let within the programme, the PSI constitutes the basis for the Security Aspects Letter.

Security Aspect Letter: means a document, issued by the appropriate authority, as part of any ESA classified contract or sub-contract, identifying requirements or those elements thereof requiring security protection.

COMPARISON OF NATIONAL SECURITY CLASSIFICATION

ESA classification	ESA TOP SECRET	ESA SECRET	ESA CONFIDENTIAL	ESA RESTRICTED
Belgium	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	Streng Geheim	Geheim	VS[1] - Vertraulich	VS – Nur für den Dienstgebrauch
Spain	Secreto	Reservado	Confidencial	Difusion limitada
France	Très Secret Défense[2]	Secret Défense	Confidentiel Défense	Diffusion restreinte
Ireland	Top Secret	Secret	Confidential	Restricted
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Netherlands	STG Zeer Geheim	STG Geheim	STG Confidentieel	
Norway	Strengt Hemmelig	Hemmelig	Konfidensielt	Begrenset
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Sweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Switzerland	Geheim Secret	Geheim Secret	Vertraulich Confidentiel	Vertraulich Confidentiel
United Kingdom	Top Secret	Secret	Confidential	Restricted

[1]Germany: VS = Verschlussache
[2] France: the classification “Très Secret Défense”, which covers governmental priority issues, may be changed only with the Prime Minister’s authorisation

Anlage 1 Teil II der Erläuterungen

ESA SECURITY REGULATIONS PART II

SECTION I

THE ORGANISATION OF SECURITY IN THE EUROPEAN SPACE AGENCY

The Director General

1. The Director General shall in consultation with the ESA Security Committee as defined in paragraphs 3 and 4 below:
   (a) implement the ESA security regulations;
   (b) consider security problems referred to him by the ESA Headquarters**,** establishments and facilities ;
   (c) examine questions involving changes in the ESA Security Regulations, in close liaison with the National Security Authority/Designated Security Authority (NSA/DSA) or any national competent authority of the Member States.
2. In particular, the Director General shall be responsible for:
   (a) Coordinating all matters of security relating to ESA activities;
   (b) Accomplishing the necessary actions in order to establish a Central ESA TOP SECRET registry to be set up in ESA Headquarters, establishments and facilities;
   (c) Addressing to the competent authorities of the Member States requests for the NSA to provide security clearances for ESA Staff members and ESA experts in accordance with Section VI;
   (d) Investigating or ordering an investigation into any leakage of ESA classified information which, on prima facie evidence, has occurred in ESA Headquarters**,** establishments or facilities;
   (e) Requesting the appropriate security authorities to initiate investigations when a leakage of ESA classified information appears to have occurred outside ESA Headquarters**,** establishments or facilities, and coordinating the enquiries when more than one security authority is involved;
   (f) Carrying out jointly and in agreement with the NSA concerned, periodic reviews of the security arrangements for the protection of ESA classified information in the Member States;
   (g) Maintaining close liaison with all security authorities concerned in order to achieve overall coordination of security;
   (h) 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.

The Security Committee

3. A Security Committee has been set up by the ESA Council Resolution (ESA/C/R/CLIX/Res.1(Final)) on 13 June 2002. This Committee should include delegates of the Member States also representing the appropriate national security authorities accompanied by such advisors as may be required. The Security Committee is chaired by a Chairman and a Vice-Chairman elected from Member States representatives.
4. The Security Committee shall, in accordance with its terms of reference, advise the ESA Council and the Director General on all issues relating to security and prepare and recommend to Council for approval decisions in this respect.

The ESA Security Office

5. In order to fulfil the responsibilities mentioned in paragraphs 1 and 2, the Director General shall have the ESA Security Office at his disposal for coordinating, supervising and implementing security measures.
6. The Head of the ESA Security Office shall advise the Director General on security matters and shall act as secretary to the Security Committee. In this regard he/she shall direct the updating of the security regulations and coordinate security measures with the competent authorities of the Member States and, as appropriate, with international organisations linked to ESA by security agreements. To that effect, he/she shall act as a liaison officer.
7. The Head of the ESA Security Office shall be responsible for the accreditation of IT systems and networks within ESA. The Head of the ESA Security Office and the relevant NSA shall jointly

decide, where appropriate, on the accreditation of IT systems and networks involving ESA Headquarters establishments and facilities on the one hand and on the other hand any other recipient of ESA classified information.

ESA headquarters, establishments and facilities

8. The Site management department shall be responsible under guidance of the ESA Security Office for the implementation of physical security measures within ESA Headquarters, establishments and facilities. The Head of the Site Management Department will nominate a member of his/her staff as being responsible to him/her in this field. This staff member is designated as a Site Security Officer.

Member States

9. Each Member State should designate a NSA responsible for the security of ESA classified information.
10. In the framework of each Member State administration, the corresponding NSA should 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 TOP SECRET, ESA SECRET and ESA CONFIDENTIAL are appropriately security cleared before they are granted access to such information;
    (e) devising such security plans as are considered necessary to prevent ESA classified information from falling into the hands of unauthorised persons.

Mutual security inspections

11. Periodic inspections of the security arrangements for the protection of ESA classified information in ESA shall be carried out by the ESA Security Office and by the NSAs concerned, jointly and in mutual agreement.

SECTION II

CLASSIFICATIONS AND MARKINGS

LEVELS OF CLASSIFICATION

Information is classified at the following levels:

1. **ESA TOP SECRET (ESA TS)**: 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.
2. **ESA SECRET (ESA S)**: 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.
3. **ESA CONFIDENTIAL (ESA C)**: 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.
4. **ESA RESTRICTED (ESA R)**: 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.

MARKINGS

5. A caveat marking may be used to specify the field covered by the document or a particular distribution on a need-to-know basis.
6. Some documents, namely related to Information Technology (IT) Systems may bear an additional marking entailing supplementary security measures as defined in the appropriate regulations and in Section XI of these regulations.

AFFIXING OF CLASSIFICATION AND MARKINGS

7. Classification and markings shall be applied as follows:
   (a) On ESA RESTRICTED documents, by mechanical or electronic means,
   (b) On ESA CONFIDENTIAL documents, by mechanical means and by hand or by printing on pre-stamped, registered paper,
   (c) On ESA SECRET and ESA TOP SECRET documents, by mechanical means and by hand.

SECTION III
CLASSIFICATION MANAGEMENT

1. Information shall be classified only when necessary. The classification shall be clearly and correctly indicated, and shall be maintained only as long as the information requires protection.
2. The responsibility for classifying information and for any subsequent downgrading or declassification rests solely with the originator. Where ESA is the originator, ESA Staff members shall classify, downgrade or declassify information only on instruction from or with the agreement of their Director or Head of Department, as appropriate.
3. 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 Director General and each Member State.

APPLICATION OF CLASSIFICATIONS

4. The classification of a document shall be determined by the level of sensitivity of its contents in accordance with the definition at Section II, paragraphs 1 to 4. It is important that classification is correctly and sparingly used. This applies especially to ESA TOP SECRET classification.
5. The originator of a document to be classified shall bear in mind the provisions set out above and curb any tendency to over- or under-classify. Although a high classification may, at first sight, appear to guarantee more protection to a document, routine over-classification can result in a loss of confidence in the validity of the classification system. On the other hand, documents shall not be under-classified with a view to avoiding the constraints connected with protection.
6. Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures of a given document may require different classifications and shall be marked accordingly. The classification of the document as a whole shall be at least that of its most highly classified part.
7. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator should indicate clearly at which level it should be classified when detached from its enclosures.

DOWNGRADING AND DECLASSIFICATION

8. ESA classified documents may be downgraded or declassified only with the prior approval of the originator and, if necessary, after discussion with other interested parties. Downgrading or declassification shall be confirmed in writing. The originator shall be responsible for informing its addressees of the change, and they in turn shall be responsible for informing any subsequent addressees, to whom they have sent or copied the document, of the change.
9. If possible, originators shall specify on classified documents a date or period when the contents may be downgraded or declassified. Otherwise, they shall keep the documents under review every five years, at the latest, in order to ensure that the original classification is necessary.

SECTION IV
PHYSICAL SECURITY

GENERAL

1. The main objective of physical security measures is to prevent an unauthorised person from gaining access to ESA classified information and/or material.
2. Complementary measures shall be taken by the Site Management Department in close liaison with the Head of the Security Office where the provisions described in this section must be reinforced in order to cover the planned activities of ESA (e.g. testing and launching related activities).

SECURITY REQUIREMENTS

3. All premises, areas, buildings, offices, rooms, communication and information systems, etc. in which ESA classified information and material is stored and/or handled shall be protected by appropriate physical security measures.
4. In deciding what degree of physical security protection is necessary, account shall be taken of all relevant factors such as:
   (a) the classification of information and/or material;
   (b) the amount and form (for example hard copy, computer storage media) of the information held;
   (c) the locally assessed threat to ESA, the Member States, and/or other institutions or third parties holding ESA classified information from, namely, sabotage, terrorism, espionage and other subversive and/or criminal activities. This threat assessment shall be undertaken by the ESA Security Office with the assistance of the Site Management Department and in close liaison with the competent national security authority where the ESA Headquarters, establishment or facility is located.
5. The physical security measures applied shall be designed to:
   (a) Deny surreptitious or forced entry by an intruder;
   (b) Deter, impede and detect actions by disloyal ESA Staff members or ESA experts (the spy within);
   (c) Prevent those ESA Staff members or ESA experts, persons working for national bodies and/or for third parties who do not have a need-to-know from having access to ESA classified information.

PHYSICAL SECURITY MEASURES

Security areas

6. Areas where information classified ESA CONFIDENTIAL or higher is handled and stored shall be so organised and structured as to correspond to one of the following:
   (a) Class I security area: an area where ESA CONFIDENTIAL or above is handled and stored in such a way that entry into the area constitutes, for all practical purposes, access to classified information.
   Such an area requires:
      (i) a clearly defined and protected perimeter through which all entry and exit is controlled;
      (ii) an entry control system, which admits only those duly cleared and specially authorised to enter the area;
      (iii) specification of the classification of the information normally held in the area, i.e. the information to which entry gives access.
   For persons who do not work in such areas, provisions shall be made for escorts or equivalent controls to prevent unauthorised access to ESA classified information and uncontrolled entry to areas subject to technical security inspections.
   (b) Class II security area: an area where ESA CONFIDENTIAL or above is handled and stored in such a way that it can be protected from access by unauthorised persons by means of internally established controls, e.g. premises containing offices in which ESA CONFIDENTIAL or above is regularly handled and stored. Such an area requires:
      (i) a clearly defined and protected perimeter through which all entry and exit is controlled;
      (ii) an entry control system which allows unescorted access only to those persons duly cleared and specially authorised to enter the area. For all other persons, provision shall be made for escorts or equivalent controls, to prevent unauthorised access to ESA classified information and uncontrolled entry to areas subject to technical security inspections.
   Areas not occupied by duty personnel on a 24-hour basis shall be inspected immediately after normal working hours to ensure that ESA classified information is properly secured.

Administrative area

7. Around or leading up to Class I or Class II security areas, an administrative area of lesser security may be established. Such an area requires a visibly defined perimeter allowing personnel and vehicles to be checked. Only ESA RESTRICTED information shall be handled and stored in such areas.

Entry and exit controls

8. Entry and exit into and from Class I and Class II security areas shall be controlled by a pass or personal recognition system. Pass systems may be supported by automated identification, which shall be regarded as a supplement to, but not a total replacement, for guards.
9. A system of visitor checks designed to deny unauthorised access to ESA classified information shall also be established. A change in the threat assessment may entail a strengthening of the entry and exit control measures, for example during the visit of prominent persons.

Guard patrols

10. Patrols of Class I and Class II security areas shall take place outside normal working hours to protect ESA assets against compromise, damage or loss. The frequency of patrols will be determined by local circumstances but shall be conducted randomly**.**

Security containers and strong rooms

11. Three classes of containers shall be used for the storage of ESA classified information:
    - Class A: containers nationally approved for storage of ESA TOP SECRET information within a Class I or a Class II security area;
    - Class B: containers nationally approved for storage of ESA SECRET and ESA CONFIDENTIAL information within a Class I or a Class II security area;
    - Class C: office furniture suitable for storage of ESA RESTRICTED information only.
12. For strong rooms constructed within a Class I or a Class II security area and for all Class I security areas where information classified ESA CONFIDENTIAL and higher is stored on open shelves or displayed on charts, maps, etc., the walls, floors and ceilings, door(s) with lock(s) shall be certified by the host NSA/DSA as offering equivalent protection to the class of security container approved for the storage of information of the same classification.

Locks

13. Locks used with security containers and strong rooms in which ESA classified information is stored shall meet the following standards:
    - Group A: nationally approved for Class A containers;
    - Group B: nationally approved for Class B containers;
    - Group C: suitable for Class C office furniture only.

Control of keys and combinations

14. Keys of security containers shall not be taken out of the office building. Combination settings of security containers shall be committed to memory by persons needing to know them. For use in an emergency, the Site Security Officer or the Head of the ESA establishment or facility shall be responsible for holding spare keys and a written record of each combination setting; the latter shall be held in separate sealed opaque envelopes. Working keys, spare security keys and combination settings shall be kept in separate security containers. These keys and combination settings should be given security protection no less stringent than the material to which they give access.
15. Knowledge of the combination settings of security containers shall be restricted to as few people as practicable. Combinations shall be reset:
    (a) on receipt of a new container;
    (b) whenever a change of personnel occurs;
    (c) whenever a compromise has occurred or is suspected;
    (d) at intervals of preferably six months and at least every 12 months.

Intrusion detection devices

16. When alarm systems, closed circuit television and other electrical devices are used to protect ESA classified information, an emergency electrical supply shall be available to ensure the continuous operation of the system if the main power supply is interrupted. Any malfunction in or tampering with such systems shall result in an alarm or other reliable warning to the surveillance personnel.

Approved equipment

17. The ESA Security Office shall maintain a list of approved security equipment based, inter alia, on information from NSAs/DSAs. The Site Management Department shall consult through the ESA Security Office with the NSA/DSA of the host Member State where the ESA Headquarters, establishment or facility is located before purchasing such equipment, as appropriate.

Physical protection of copying and telefax machines

18. Copying and telefax machines shall be physically protected to the extent necessary to ensure that only authorised persons can use them and that all classified products are subject to proper controls.

PROTECTION AGAINST OVERLOOKING AND EAVESDROPPING

Overlooking

19. All appropriate measures shall be taken by day and by night to ensure that ESA classified information is not seen, even accidentally, by any unauthorised person.

Eavesdropping

20. Offices or areas in which information classified ESA SECRET and above is regularly discussed shall be protected against passive and active eavesdropping attacks where the risk demands it. The assessment of the risk of such attacks shall be the responsibility of the ESA Security Office after consultation, as necessary, with NSAs/DSAs.
21. It is not permitted to introduce mobile phones, private computers, recording devices, cameras and other electronic or recording devices into security areas or technically secure areas without the prior authorisation from the Head of the Security Office.
22. To determine the protective measures to be taken in premises sensitive to passive eavesdropping (e.g. insulation of walls, doors, floors and ceilings, measurement of compromising emanations) and to active eavesdropping (e.g. search for microphones), the ESA Security Office may request assistance from experts from the host NSA/DSA. Site security officers of ESA Headquarters, establishments or facilities may request technical inspections to be carried out by the ESA Security Office and/or with the assistance from experts from the host NSA/DSA.
23. Likewise, when circumstances require, the telecommunications equipment and the electrical or electronic office equipment of any kind used during meetings at ESA SECRET level and above may be checked by technical security specialists of NSAs/DSAs at the request of the Head of the ESA Security Office. Such checks will be carried out in close liaison with the Site Management Department.

TECHNICALLY SECURE AREAS

24. Certain areas may be designated as technically secure areas. A special entry check shall be carried out. Such areas shall be kept locked by an approved method when not occupied and all keys treated as security keys. Such areas shall be subject to regular physical inspections, carried out by the Site Management Department under guidance of the ESA Security Office. Inspections will also be undertaken following any unauthorised entry or suspicion of such an entry.
25. A detailed inventory of equipment and furniture shall be maintained. No item of furniture or equipment shall be brought into such an area until it has undergone a careful inspection by specially trained security personnel, designed to detect any listening devices. As a general rule, the installation of communication lines in technically secure areas should be avoided.

SECTION V
ACCESS TO ESA CLASSIFIED INFORMATION

1. Access to ESA classified information will be authorised only for persons having a “need-to-know” for carrying out their duties or missions. Access to ESA TOP SECRET, ESA SECRET and ESA CONFIDENTIAL will be authorised only for persons in possession of the appropriate security clearance.
2. A list of the posts requiring access to ESA classified information shall be drawn up by the ESA Security Office. The responsibility for determining the “need-to-know” will rest with the Director General, the Head of ESA Headquarters, establishments or facilities and with the national body in which the person concerned is to be employed, according to the requirements of the task.
3. The Personnel security clearance will be the responsibility of the competent national authority of the Member States based on relevant applicable procedures. This will result in the issue of a “Personnel security clearance certificate” showing the highest level of ESA classified information to which the cleared person may have access and the date of expiry.
4. Employees of ESA contractors working for infrastructure and support services within ESA Headquarters, establishments or facilities who for the requirement of their task may have access on the need-to-know basis to ESA classified information shall be appropriately security cleared in compliance with the provisions set out in this Section.

5. When persons not having an established “need-to-know” are to be employed in circumstances in which they may have access to ESA classified information (e.g. messengers, security agents, maintenance personnel and cleaners, etc…) they shall first be appropriately security cleared in compliance with the provisions set out in this Section.
6. Persons other than ESA Staff members or ESA experts and persons other than officials or other servants of Member States, with whom it may occasionally be necessary to discuss, or to whom it may be necessary to show, ESA classified information, must have a valid personnel security clearance as regards classified information and be briefed as to their responsibility for its security.
7. Persons who have access to ESA classified information shall be informed of the consequences of any breach of security and compromise of ESA classified information as set out in Section X of these security regulations.

SPECIFIC RULES ON ACCESS TO ESA TOP SECRET INFORMATION

8. All persons who are required to have access to ESA TOP SECRET information shall be designated by the Head of their department and their names kept in the appropriate ESA TOP SECRET registry.
9. Before having access to ESA TOP SECRET information, all persons shall sign a certificate to the effect that they have been briefed on ESA security procedures and that they fully understand their special responsibility for safeguarding ESA TOP SECRET information, and the consequences which the ESA rules and national law or administrative rules provide when classified information passes into unauthorised hands, either by intent or through negligence.
10. In the case of persons required to access ESA TOP SECRET information at meetings, etc., the competent Security Officer of the service or body in which that person is employed shall provide confirmation to the body organising the meeting that the persons concerned have been appropriately security cleared.
11. The names of all persons ceasing to be employed on duties requiring access to ESA TOP SECRET information shall be removed from the ESA TOP SECRET list. In addition, the attention of all such persons shall be drawn again to their special responsibility for the safeguarding of ESA TOP SECRET information. They shall also sign a declaration stating that they will neither use nor pass on ESA TOP SECRET information in their possession.

SPECIFIC RULES ON ACCESS TO ESA SECRET AND ESA CONFIDENTIAL INFORMATION

12. All persons who are to have access to ESA SECRET or ESA CONFIDENTIAL information shall be acquainted with the appropriate security regulations and shall be aware of the consequences of negligence.
13. In the case of persons having access to ESA SECRET or ESA CONFIDENTIAL information at meetings, etc., the Security Officer of the body in which that person is employed shall notify the body organising the meeting that the persons concerned have such authorisation.

SPECIFIC RULES ON ACCESS TO ESA RESTRICTED INFORMATION

14. Persons with access to ESA RESTRICTED information shall be made aware of these security regulations and of their responsibilities regarding its protection and of the consequences of negligence.

TRANSFERS

15. When a person is transferred from a post which involves the handling of ESA classified material, the Registry will oversee the proper transfer of that material from the outgoing to the incoming person.

SPECIAL INSTRUCTIONS

16. Persons who are required to handle ESA classified information should, on first taking up their duties and periodically thereafter, be made aware of:
    (a) The dangers to security arising from indiscreet conversation;
    (b) Precautions to take in their relations with the press and with representatives of special interest groups;
    (c) The threat presented by, amongst others, espionage activities from intelligence services or private industry, sabotage, terrorism or the actions of subversive and/or criminal groups, which may target ESA and its Member States as regards ESA classified information or activities;

(d) The obligation to report immediately to the appropriate security authorities any approach or manoeuvre giving rise to suspicions of espionage activity or any unusual circumstances relating to security.

17. All persons normally exposed to frequent contact with representatives of countries who may target ESA and Member States as regards ESA classified information and activities shall be given a briefing on the techniques known to be employed by various intelligence services.
18. There are no ESA security regulations concerning private travel to any destination by persons cleared for access to ESA classified information. The competent security authorities will, however, acquaint the persons falling within their responsibility with travel regulations to which they may be subject. It will be the responsibility of the security officers to arrange refresher meetings for persons concerned on these special instructions.

SECTION VI

SECURITY CLEARANCE PROCEDURE FOR ESA STAFF MEMBERS AND ESA EXPERTS

1. Only ESA Staff members and ESA experts who, by reason of their duties and for the requirements of their task, need to have knowledge of, or to use, ESA classified information, shall have access to such information provided they have been appropriately security cleared by the competent national authority.
2. In order to have access to information classified as ESA TOP SECRET, ESA SECRET and ESA CONFIDENTIAL, ESA Staff members and ESA experts must hold a Personnel Security Clearance (PSC) granted by the competent national authorities of the Member States (National Security Authority or equivalent national authority).
3. The PSC shall be valid for a period not exceeding five years for ESA TOP SECRET and ten years for ESA SECRET and ESA CONFIDENTIAL. The authorisation for access given on the basis of this PSC shall not exceed the duration of the tasks on the basis of which it was granted.
4. Security clearance procedure shall be carried out with the assistance of the ESA Staff member or ESA expert concerned and at the request of the Director General by the competent national authorities of the Member State of which this Staff member or expert is a national. Should the Staff member or the ESA expert reside in the territory of another Member State, the competent national authorities may secure the cooperation of the authorities of the State of residence.
5. As part of the security clearance procedure, the ESA Staff member or ESA expert concerned shall be required to complete a personal information form and to acknowledge that he/she understands that any breach of ESA security may result in his/her ESA immunity being waived.
6. The Director General shall specify in his request the type and level of classified information to be made available to the ESA Staff member or ESA expert concerned, so that the NSA/DSA or national competent authorities can carry out the security clearance procedure.
7. The whole security clearance procedure together with the results obtained shall be subject to the relevant rules and regulations in force in the Member State concerned, including those concerning appeals.
8. Where the competent NSA/DSA of the Member State grants a Personnel security clearance certificate, the Director General may grant the ESA Staff member or ESA expert concerned authorisation for access to classified information provided this Staff member or expert has the need to know.
9. A denial by the NSA/DSA to grant a Personnel security clearance certificate shall be notified by the Director General to the ESA Staff member or ESA expert concerned, who may ask to be heard by the Director General. The Director General shall ask the competent national authority for any further clarification they can provide in compliance with their national rules and regulations. If the denial is confirmed by the NSA/DSA authorisation shall not be granted.
10. All ESA Staff members and ESA experts granted a PSC shall, at the time the PSC is granted and at regular intervals thereafter, receive any necessary instructions concerning the protection of classified information and the means of ensuring such protection. Such persons shall sign a declaration acknowledging receipt of the instructions and give an undertaking to obey them.
11. Authorisation to access ESA classified information shall be withdrawn by the Director General if the relevant NSA/DSA withdraws the Security Clearance. Any decision to withdraw authorisation shall be notified to the ESA Staff member or ESA expert concerned, who may ask to be heard by the Director General. The Director General may ask the competent national

authority for any further clarification they can provide in compliance with their national rules and regulations.

12. The Director General shall take any measure necessary in order to implement this section, in particular as regards the rules governing access to the list of cleared ESA Staff members or experts.
13. Exceptionally, pending the outcome of the security clearance procedure, the Director General may, with the written agreement of the NSA/DSA or national competent authority, grant temporary access authorisation for information classified up to and including ESA SECRET only, for a period not exceeding six months, to an ESA staff member.
14. The provisional and temporary authorisations thus granted shall not give access to ESA TOP SECRET information; such access shall be limited to ESA Staff members who have been granted a PSC for this classification. Pending the outcome of the security clearance procedure, ESA Staff members for whom clearance at ESA TOP SECRET level has been requested may be authorised temporarily and provisionally to access information classified up to and including ESA SECRET.

SECTION VII

PREPARATION, DISTRIBUTION, TRANSMISSION, STORAGE AND DESTRUCTION OF ESA CLASSIFIED MATERIAL

General provisions

This section details measures for the preparation, distribution, transmission, storage and destruction of ESA classified documents. It shall be used as a reference for the adaptation of those measures for other ESA classified material, according to its type and on a case-by-case basis.

Chapter I

Preparation and distribution of ESA classified documents

PREPARATION

1. The ESA classifications and markings shall be applied as established in Section II and appear at the top and bottom centre of each page, and each page shall be numbered. Each ESA classified document shall bear a reference number and a date. In the case of ESA TOP SECRET and ESA SECRET documents, this reference number shall appear on each page. If they are to be distributed in several copies, each one shall bear a copy number, which will appear on the first page, together with the total number of pages. All annexes and enclosures shall be listed on the first page of a document classified ESA CONFIDENTIAL and above.
2. Documents classified ESA CONFIDENTIAL and above shall be typed, translated, stored, photocopied, reproduced magnetically or microfilmed only by persons who have been cleared for access to ESA classified information up to at least the appropriate security classification of the document in question.

The provisions regulating the computerised production of classified documents are set out in Section XI.

DISTRIBUTION

3. ESA classified information shall be distributed only to persons with a need to know and having the appropriate security clearance. The initial distribution shall be specified by the originator.
4. ESA TOP SECRET documents shall be circulated through ESA TOP SECRET registries (see Section VIII). In the case of ESA TOP SECRET messages, the competent registry may authorise the Head of the communications centre to produce the number of copies specified in the list of addressees.
5. Documents classified ESA SECRET shall be circulated through registries. They may be redistributed by the original addressee to other addressees based on a need to know. The originating authorities shall, however, clearly state any caveats they wish to impose. Whenever such caveats are imposed, the addressees may redistribute the documents only with the originating authorities' authorisation.
6. Every document classified ESA CONFIDENTIAL shall, on arriving at or leaving an establishment, be recorded by the establishment's registry. The particulars to be entered (references, date and where applicable the copy number) shall be such as to identify the documents and be entered into a logbook or in special protected computer media.

Chapter II
Transmission of ESA classified documents

PACKAGING

7. Documents classified ESA CONFIDENTIAL and above shall be transmitted in heavy duty, opaque double envelopes. The inner envelope shall be marked with the appropriate ESA security classification as well as, if possible, full particulars of the recipient's job title and address.
8. Only a Registry Control Officer, or his substitute, may open the inner envelope and acknowledge receipt of the documents enclosed, unless that envelope is addressed to an individual. In such a case, the appropriate Registry shall log the arrival of the envelope, and only the individual to whom it is addressed may open the inner envelope and acknowledge receipt of the documents it contains.
9. A receipt form shall be placed in the inner envelope. The receipt, which will not be classified, should quote the reference number, date and copy number of the document, but never its subject.
10. The inner envelope shall be enclosed in an outer envelope bearing a package number for receipting purposes. Under no circumstances shall the security classification appear on the outer envelope.
11. For documents classified ESA CONFIDENTIAL and above, couriers and messengers shall obtain receipts against the package numbers.

TRANSMISSION WITHIN A BUILDING OR GROUP OF BUILDINGS

12. Within a given building or group of buildings, classified documents may be carried in a sealed envelope bearing only the addressee's name, on condition that it is carried by a person cleared to the level of classification of the documents.

TRANSMISSION OF ESA DOCUMENTS WITHIN A COUNTRY

13. Within a country, ESA TOP SECRET documents should be sent only by means of official courier or by persons authorised to have access to ESA TOP SECRET information.
14. Whenever an official courier is used for the transmission of a ESA TOP SECRET document outside the confines of a building or group of buildings, the packaging and receipting provisions contained in this Chapter shall be complied with. Delivery services shall be so staffed as to ensure that packages containing ESA TOP SECRET documents remain under the direct supervision of a responsible official at all times.
15. Exceptionally, ESA TOP SECRET documents may be taken by authorised persons, other than official couriers, outside the confines of a building or group of buildings for local use at meetings and discussions, provided that:
    (a) The bearer is authorised to have access to those ESA TOP SECRET documents;
    (b) The mode of transportation complies with national rules governing the transmission of national TOP SECRET documents;
    (c) Under no circumstances does the official leave the ESA TOP SECRET documents unattended;
    (d) Arrangements are made for the list of documents so carried to be held in the ESA TOP SECRET Registry holding the documents and recorded in a log, and checked against this record on their return.
16. Within a country, ESA SECRET and ESA CONFIDENTIAL documents may be sent either by post, if such transmission is permitted under national regulations and is in accordance with the provisions of those regulations, or by official couriers or by persons cleared for access to ESA classified information.
17. Each Member State and ESA should prepare instructions on the personal carrying of ESA classified documents based on these regulations. The bearer should be required to read and sign these instructions. In particular, the instructions should make it clear that, under no circumstances, may documents:
    (a) Leave the bearer's possession unless they are in safe custody in accordance with the provisions contained in Section IV;
    (b) Be left unattended in public transport or private vehicles, or in places such as restaurants or hotels. They may not be stored in hotel safes or left unattended in hotel rooms;
    (c) Be read in public places such as aircraft or trains.

TRANSMISSION FROM THE TERRITORY OF ONE MEMBER STATE TO THE TERRITORY OF ANOTHER

18. Material classified ESA CONFIDENTIAL and above should be conveyed from one Member State to another by diplomatic pouch.
19. However, the personal carriage of material classified ESA SECRET and ESA CONFIDENTIAL may be permitted if provisions for the carriage are such as to ensure that they cannot fall into any unauthorised person's hands.
20. NSAs/DSAs may authorise personal carriage when diplomatic pouch is not available or the use of such couriers would result in a delay that would be detrimental to ESA activities and the material is urgently required by the intended recipient. Each Member State should prepare instructions covering the personal carriage of material classified up to and including ESA SECRET internationally by persons other than diplomatic pouch. The instructions should require that:
    (a) The bearer has the appropriate security clearance granted by Member States;
    (b) A record is held in the appropriate office or registry of all material so carried;
    (c) Packages or bags containing ESA material bear an official seal to prevent or discourage inspection by customs, and labels with identification and instructions to the finder;
    (d) The bearer carries a courier certificate and/or mission order recognised by all ESA States authorising him to carry the package as identified;
    (d) No ESA non-Member State or its frontier is crossed when travelling overland unless the shipping State has a specific guarantee from that State;
    (f) The bearer's travel arrangements with regard to destinations, routes to be taken and means of transportation to be used will be in accordance with ESA Regulations or - if national regulations with respect to such matters are more stringent - in accordance with such regulations;
    (g) The material must not leave the possession of the bearer unless it is housed in accordance with the provisions for safe custody contained in Section IV;
    (h) The material must not be left unattended in public or private vehicles, or in places such as restaurants or hotels. It must not be stored in hotel safes or left unattended in hotel rooms;
    (i) If the material being carried contains documents, these must not be read in public places (for example in aircraft, trains, etc.).

    The person designated to carry the classified material must read and sign a security briefing that contains, as a minimum, the instructions listed above and procedures to be followed in an emergency or in case the package containing the classified material is challenged by customs or airport security officials.

TRANSMISSION OF ESA RESTRICTED DOCUMENTS

21. ESA RESTRICTED items will normally be transmitted in a single envelope not bearing a classification by:
    a) a normal or registered mail, as appropriate;
    b) commercial courrier services;
    c) hand carriage by staff members without formal courier order. During travel, the items must remain under permanent personal custody and may not be left unattended in hotel rooms or vehicles and may not be read in public.

COURIER PERSONNEL SECURITY

22. All couriers and messengers employed to carry ESA SECRET and ESA CONFIDENTIAL documents shall be appropriately security cleared.

Chapter III

Transmission through information technology and information systems

23. Communications security measures are designed to ensure the secure transmission of ESA classified information. The detailed rules applicable to the transmission of such ESA classified information are dealt with in Section XI.
24. Only accredited communications centres and networks and/or terminals and systems may transmit information classified ESA CONFIDENTIAL and ESA SECRET.

Chapter IV

Extra copies and translations of and extracts from ESA classified documents

25. Only the originator may authorise the copy or translation of ESA TOP SECRET documents.
26. If persons without ESA TOP SECRET clearance require information which, although contained in a ESA TOP SECRET document, does not have that classification, the Head of the ESA TOP SECRET Registry may be authorised to produce the necessary number of extracts from that document. He/she shall, at the same time, take the necessary steps to ensure that these extracts are given the appropriate security classification.
27. Documents classified ESA SECRET and lower may be reproduced and translated by the addressee, within the framework of the national security regulations and on condition that it complies strictly with the need-to-know principle. The security measures applicable to the original document shall also be applicable to reproductions and/or translations thereof.

Chapter V

Musters and checks, storage and destruction of ESA classified documents

MUSTERS AND CHECKS

28. Every year, each ESA TOP SECRET Registry as referred to in Section VIII shall carry out an itemised muster of ESA TOP SECRET documents in accordance with the regulations set out in Section VIII, (9) to (11). ESA classified documents below the level of ESA TOP SECRET shall be subject to internal checks in accordance with national guidelines, and, in the case of the ESA, according to instructions from the Director General.
    These operations shall afford the opportunity to secure holders' views as to:
    (a) The possibility of downgrading or declassifying certain documents;
    (b) Documents to be destroyed.

ARCHIVE STORAGE OF ESA CLASSIFIED INFORMATION

29. 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 archiving of classified information shall be consistent with ESA records and archive management policy and procedures.
30. To minimise storage problems, the Control Officers of all registries shall be authorised in consultation with the ESA Records Manager to have ESA SECRET, ESA CONFIDENTIAL and ESA RESTRICTED documents microfilmed or otherwise stored in magnetic or optical media for archive purposes, providing that:
    a) The microfilming/storage process is undertaken by personnel with current clearance for the corresponding appropriate classification level;
    b) The microfilm/storage medium is afforded the same security as the original documents;
    c) Rolls of film, or other type of support, contain only documents of the same ESA SECRET, ESA CONFIDENTIAL or ESA RESTRICTED classification level;
    d) The microfilming/storing of ESA SECRET document is clearly indicated in the record used for the annual inventory;
    e) ESA original documents, which have been microfilmed or otherwise stored are destroyed in accordance with the regulations set out in paragraphs 33 to 37.
31. ESA Staff members or ESA experts, when leaving the Agency or before transfer to another service/or site must hand over all records in their custody through the appropriate registry as provided for in Section V, paragraph 14.
32. These rules also apply to any other form of storage authorised by the NSA/DSA, such as electromagnetic media and optical disk.

ROUTINE DESTRUCTION OF ESA CLASSIFIED DOCUMENTS

33. To prevent the unnecessary accumulation of ESA classified documents, those regarded by the Directorate or Head of Department, as appropriate, holding them as out of date, except for those having long-term value and which are handled as such as ESA archives (see previous paragraphs on archive storage), or surplus in number shall be destroyed according to their level of classification.
34. ESA TOP SECRET documents shall be destroyed in the following manner:

(a) ESA TOP SECRET documents shall be destroyed only by the Central Registry responsible for them. Each document destroyed shall be listed in a destruction certificate, signed by the ESA TOP SECRET Control Officer and by the Officer witnessing the destruction, who shall be ESA TOP SECRET cleared. A note to this effect shall be made in the logbook;

(b) The registry shall keep the destruction certificates, together with the distribution sheets, for a period of ten years. Copies shall be forwarded to the originator or to the appropriate central registry only when explicitly requested;

(c) ESA TOP SECRET documents, including all classified waste resulting from the preparation of ESA TOP SECRET documents such as spoiled copies, working drafts, typed notes, floppy disks, shall be destroyed, under the supervision of a ESA TOP SECRET Registry Control Officer, by burning, pulping, shredding or otherwise reducing into an unrecognisable and non-reconstitutable form.

35. ESA SECRET documents shall be destroyed by the registry responsible for those documents, under the supervision of a security cleared person, using one of the processes indicated in paragraph 34(c). ESA SECRET documents that are destroyed shall be listed on signed destruction certificates to be retained by the Registry, together with the distribution forms, for at least three years.

36. ESA CONFIDENTIAL documents shall be destroyed by the registry responsible for those documents, under the supervision of a security cleared person, by one of the processes indicated in paragraph 34(c). Their destruction shall be recorded in accordance with national regulations and, in the case of ESA, according to instructions from the Director General.

37. ESA RESTRICTED documents shall be destroyed in accordance with national regulations and, in the case of ESA, according to instructions from the Director General.

DESTRUCTION IN EMERGENCIES

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

39. The arrangements for the safeguarding and/or destruction of ESA SECRET and ESA CONFIDENTIAL material in a crisis shall under no circumstances adversely affect the safeguarding or destruction of ESA TOP SECRET material, including the enciphering equipment, whose treatment shall take priority over all other tasks. The measures to be adopted for the safeguarding and destruction of enciphering equipment in an emergency shall be covered by ad hoc instructions.
Instructions need to be available on the spot in a sealed envelope. Means/tools for destruction must be available.

CHAPTER VI

Specific rules applicable to documents intended for the ESA Council

40. Within ESA Headquarters, a “Classified Information Office” shall monitor information classified as ESA SECRET or ESA CONFIDENTIAL contained in documents for the ESA Council.
Under the authority of the Director General it shall:

(a) Manage operations relating to the registration, reproduction, translation, transmission dispatch and destruction of such information;

(b) Update the list of particulars on classified information;

(c) Periodically question issues on the need to maintain the classification of information;

(d) Lay down, in collaboration with the ESA Security Office, the practical arrangements for classifying and declassifying information.

41. The Classified Information Office shall keep a register of the following particulars:

(a) The date of preparation of the classified information;

(b) The level of classification;

(c) The expiry date of the classification;

(d) The name and department of the issuer;

(e) The recipient or recipients, with serial number;

(f) The subject;

(g) The number;

(h) The number of copies circulated;

(i) The preparation of inventories of the classified information submitted to the Council;

(j) The register of declassification and downgrading of classified information.

42. The general rules provided for in Chapters I to V of this Section shall apply to the Classified Information Office of the ESA Headquarters, unless modified by the specific rules laid down in this Chapter.

SECTION VIII
ESA CENTRAL REGISTRIES

ESA TOP SECRET REGISTRIES

1. A Central ESA TOP SECRET Registry will ensure the recording, handling and distribution of ESA TOP SECRET documents in accordance with these security regulations. The head of the ESA TOP SECRET Registry in ESA, respectively in each Member State, will be the ESA TOP SECRET Registry Control Officer.
2. The Central ESA TOP SECRET Registry will act as the main receiving and despatching authority in ESA, as well as, if appropriate, in Member States, international organisations and third States with which ESA has agreements on security procedures for the exchange of classified information.
3. When necessary, sub-registries shall be established, to be responsible for the internal management of ESA TOP SECRET documents; they shall keep up-to-date records of the circulation of each document held on the sub-registry's charge.
4. ESA TOP SECRET sub-registries shall be set up as specified in Section I paragraph 2. b) in response to long term needs and shall be attached to a central ESA TOP SECRET registry. If there is a need to consult ESA TOP SECRET documents only temporarily and occasionally, these documents may be released without setting up a ESA TOP SECRET sub-registry provided rules are laid down to ensure that they remain under the control of the appropriate ESA TOP SECRET registry and that all physical and personnel security measures are observed.
5. Sub-registries may not transmit ESA TOP SECRET documents direct to other sub-registries of the same central ESA TOP SECRET registry without express approval by the latter.
6. All exchanges of ESA TOP SECRET documents between sub-registries not attached to the same central registry shall be routed through the central ESA TOP SECRET registries.

THE CENTRAL ESA TOP SECRET REGISTRY

7. As the Control Officer, the head of the central ESA TOP SECRET registry shall be responsible for:
   (a) The transmission of ESA TOP SECRET documents in accordance with the regulations defined in Section VII;
   (b) Maintaining a list of all its dependent ESA TOP SECRET sub-registries together with names and signatures of the appointed Control Officers and their authorised deputies;
   (c) Holding receipts from registries for all ESA TOP SECRET documents distributed by the Central Registry;
   (d) Maintaining a record of ESA TOP SECRET documents held and distributed;
   (e) Maintaining an up-to-date list of all central ESA TOP SECRET Registries with which he/she normally corresponds, together with the names and signatures of their appointed Control Officers and their authorised deputies;
   (f) The physical safeguarding of all ESA TOP SECRET documents held within the registry in accordance with Section IV of these regulations.

ESA TOP SECRET SUB-REGISTRIES

8. As the Control Officer, the head of a ESA TOP SECRET sub-registry shall be responsible for:
   (a) The transmission of ESA TOP SECRET documents in accordance with regulations contained in Section VII and paragraphs 5 and 6 of Section VIII;
   (b) Maintaining an up-to-date list of all persons authorised to have access to the ESA TOP SECRET information under his control;

(c) The distribution of ESA TOP SECRET documents in accordance with the instructions of the originator or on a need-to-know basis, having first checked that the addressee has the requisite security clearance;

(d) 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 registries and holding all corresponding receipts;

(e) Maintaining an up-to-date list of ESA TOP SECRET registries with whom he is authorised to exchange ESA TOP SECRET documents, together with the names and signatures of their control officers and authorised deputies;

(f) The physical safeguarding of all ESA TOP SECRET documents held within the sub-registry in accordance with the regulations laid down in Section IV.

INVENTORIES

9. Every twelve months, each ESA TOP SECRET registry shall carry out an itemised inventory of all ESA TOP SECRET documents for which it is accountable. A document is deemed to have been accounted for if the registry physically musters the document, or holds a receipt from the ESA TOP SECRET registry to which the document has been transferred, a destruction certificate for the document or an instruction to downgrade or declassify that document.
10. ESA TOP SECRET Sub-registries shall forward the findings of their annual inventory to the Central Registry to which they are answerable, on a date specified by the latter.
11. NSAs/DSAs, as well as those ESA establishments and international organisations in which a central ESA TOP SECRET registry has been set up, shall forward the findings of the annual inventories conducted in central ESA TOP SECRET registries to the Director General, by 1 April each year at the latest.

SECTION IX

SECURITY MEASURES TO BE APPLIED AT THE TIME OF SPECIFIC MEETINGS HELD OUTSIDE ESA HEADQUARTERS, ESTABLISHMENTS AND FACILITIES AND INVOLVING HIGH SENSITIVITY ISSUES

GENERAL

1. When ESA Council, at Ministerial level, or other important meetings, are held outside ESA Headquarters in Paris, or outside establishments or facilities, and where justified by the particular security requirements relating to the high sensitivity of the issues or information dealt with, the security measures described below should be taken. These measures concern only the protection of ESA classified information; other security measures may have to be planned.

RESPONSIBILITIES

Hosting Member States

2. The Member State on whose territory the meeting is being held (the hosting Member State) should be responsible, in cooperation with the ESA Security Office, for the security of the ESA Council at Ministerial level or other important meetings.
   As regards the protection of security, it should specifically ensure that:

(a) Plans are drawn up to deal with security threats and security-related incidents, the measures in question covering in particular the safe custody of ESA classified documents in offices;

(b) Measures are taken to provide possible access to ESA Council's communications system for the receipt and transmission of ESA classified messages. The host Member State will also provide access if required to secure telephone systems.

Member States

3. The Member States' authorities should take the necessary steps to ensure that:

(a) Appropriate security clearance certification is provided for their national delegates, if necessary by signal or fax, either directly to the Meeting Security Officer or via the ESA Security Office;

(b) Any specific threat is made known to the host Member State's authorities and, as appropriate, to the ESA Security Office so that appropriate action can be taken.

Meeting Security Officer

4. A Security Officer shall be appointed and be responsible for the general preparation and control of general internal security measures and for coordination with the other security authorities concerned.

ESA Security Office

5. The ESA Security Office should act as an adviser on security for the preparation of the meeting; it should be represented there to help and advise the Meeting security officer and delegations as necessary.

SECURITY MEASURES

Security areas

6. The following security areas should be established:
   (a) A Class II security area, consisting of a drafting room, the ESA offices and reprographic equipment, as well as delegations' offices as appropriate;
   (b) A Class I security area, consisting of the conference room and interpreters' and sound engineers' booths;
   (c) Administrative areas, consisting of the press area and those parts of the meeting place that are used for administration, catering and accommodation, as well as the area immediately adjacent to the Press Centre and the meeting place.

Passes

7. The Meeting Security Officer should issue appropriate badges as requested by the delegations, according to their needs. Where required, a distinction may be made as regards access to different security areas.

Control of photographic and audio equipment

8. Except for the official recordings, no camera or recording equipment, including cellular phones may be brought into a Class I security area, with the exception of equipment brought by photographers and by sound engineers duly authorised by the Meeting Security Officer.

Inspection of offices

9. The Meeting Security Officer shall arrange for the ESA Executive and delegations' offices to be inspected at the end of each working day to ensure that all ESA classified documents are being kept in a safe place; if not, he/she shall take the requisite measures.

Disposal of ESA classified waste

10. All waste should be treated as ESA classified, and waste-paper baskets or bags shall be given to the ESA Executive and delegations for its disposal. Before leaving the premises they have been assigned, the ESA Executive and delegations shall take their waste to the meeting security officer, who shall arrange for its destruction according to these regulations.

SECTION X

BREACHES OF SECURITY AND COMPROMISE OF ESA CLASSIFIED INFORMATION

1. A breach of security occurs as the result of an act or omission contrary to an ESA or national security regulation, which might endanger or compromise ESA classified information.
2. Compromise of ESA classified information occurs when it has wholly or in part fallen into the hands of unauthorised persons, i.e. 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.
3. ESA classified information may be compromised as a result of carelessness, negligence or indiscretion as well as by the activities of services which target ESA or its Member States, as regards ESA classified information and activities, or by subversive organisations.
4. It is important that all persons who are required to handle ESA classified information are thoroughly briefed on security procedures, the dangers of indiscreet conversation and their relationships with the press. They should be aware of the importance of reporting any breach of security, which may come to their notice at once to the competent security authority of the Member State, the Security Officer of ESA headquarters, establishment or facility in which they are employed.

5. When a security authority discovers or is informed of a breach of security relating to ESA classified information or of the loss or disappearance of ESA classified material, it shall take timely action in order to:
   (a) Safeguard evidence
   (b) Establish the facts;
   (c) Assess and minimise the damage done;
   (d) Prevent a recurrence;
   (e) Notify the appropriate authorities of the effects of the breach of security.
   In this context, the following information shall be provided:
      (i) A description of the information involved, including its classification, reference and copy number, date, originator, subject and scope;
      (ii) A brief description of the circumstances of the breach of security, including the date and the period during which the information was exposed to compromise;
      (iii) A statement of whether the originator has been informed.
6. It shall be the duty of each security authority, as soon as it is notified that such a breach of security may have occurred, to report the fact immediately to the ESA Security Office. In the event of a compromise of ESA classified information occurring within the jurisdiction of a Member State, it shall be reported to the ESA Security Office as specified in paragraph 5, through the NSA/DSA responsible.
7. Cases involving ESA RESTRICTED information need to be reported only when they present unusual features.
8. On being informed that a breach of security has occurred, the Director General shall:
   (a) Notify the authority that originated the classified information in question;
   (b) Ask the appropriate security authorities to initiate investigations;
   (c) Coordinate enquiries where more than one security authority is affected;
   (d) Obtain a report on the circumstances of the breach, the date or period during which it may have occurred and was discovered, with a detailed description of the content and classification of the material involved. Damage done to the interests of ESA or of one or more of its Member States and action taken to prevent a recurrence should also be reported.
9. The originating authority shall inform the addressees and shall give appropriate instructions.
10. Any individual who is responsible for compromising ESA classified information shall be liable to disciplinary action according to the relevant rules and regulations. Such action shall be without prejudice to any other legal action. ESA staff members and ESA experts shall be informed about the possible legal consequences of breaches of security and in particular about Article 7 of the ESA Security Agreement on the possible waiver of immunity.

SECTION XI

PROTECTION OF ESA CLASSIFIED INFORMATION HANDLED IN INFORMATION TECHNOLOGY AND COMMUNICATION SYSTEMS

Chapter I

Introduction

GENERAL ASPECTS

1. The security policy and requirements in this section shall apply to all communications and information systems and networks (hereinafter Systems) handling ESA classified information.
2. All Systems require security measures to protect the integrity and availability of those Systems and of the information they contain. In addition, Systems containing ESA classified information require security measures to protect the confidentiality of such information. The security measures to be applied to those Systems will be determined by the designated Security Accreditation Authority (SAA) and will be commensurate with the assessed risk and consistent with the policy stated in these security regulations.
   The IT security policy applied by ESA has the following elements:
   - It forms an integral part of security in general, and complements all elements of information security, personnel security and physical security;

- Division of responsibilities between technical System owners, owners of ESA classified information stored or handled in technical Systems, IT security specialists and users;
- Description of security principles and requirements of each IT System;
- Approval of these principles and requirements by a designated Security Accreditation authority (SAA);
- Taking into account the specific threats and vulnerabilities in the IT area.

3. Protection embedded IT Systems shall be determined and specified in the general context of the Systems to which they belong using applicable provisions of this section to the extent possible.

THREATS TO, AND VULNERABILITIES OF SYSTEMS

4. In general terms, a threat can be defined as a potential for the accidental or deliberate compromise of security. In the case of Systems, such a compromise involves loss of one or more of the properties of confidentiality, of integrity and of availability. A vulnerability can be defined as a weakness or lack of controls that would facilitate or allow a threat actuation against a specific asset or target. 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.
5. ESA classified and unclassified information handled in Systems in a concentrated form designed for rapid retrieval, communication and use is vulnerable to many risks (defined as a combination of threats and vulnerabilities). These include access to the information by unauthorised users or, conversely, denial of access to authorised users. There are also the risks of the unauthorised disclosure, corruption, modification or deletion of the information. Furthermore, the complex and sometimes fragile equipment is expensive and often difficult to repair or replace rapidly. These Systems are therefore attractive targets for intelligence gathering operations and sabotage, especially if security measures are thought to be ineffective.

SECURITY MEASURES

6. 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 ESA classified information, the appropriate standards of conventional security shall be applied according to the level of ESA classified information to be protected, along with appropriate special security procedures and techniques particularly designed for each System.
7. 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.
8. Computer security measures (hardware and software security features) 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 requirement. The process of accreditation shall determine that an adequate level of assurance is present to support this reliance on computer security measures.

SYSTEM-SPECIFIC SECURITY REQUIREMENT STATEMENT (SSRS)

9. For all Systems handling information classified ESA CONFIDENTIAL and above, a System-specific security requirement statement (SSRS) shall be required to be produced by the IT System Operational Authority (ITSOA)/its Technical System Owner (TSO) and the Information Owner in cooperation with input and assistance as required from the project staff and the relevant INFOSEC Authority, and approved by the Security Accreditation Authority (SAA). An SSRS shall also be required where the confidentiality, availability or integrity of the ESA RESTRICTED or unclassified information is deemed critical by the appropriate SAA.
10. The SSRS shall be formulated at the earliest stage of a 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.
11. The SSRS shall form the binding agreement between the IT System Operational Authority/Technical System Owner and the Information Owner and the SAA against which the System is to be accredited.
12. The SSRS 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, or imposed by parameters covering the operational environment, the security mode of operation or user requirements. The SSRS is an integral part of project documentation submitted to the appropriate authorities for technical, budgetary and security approval purposes. In its final form, the SSRS constitutes a complete statement of what it means for the System to be secure.

SECURITY MODES OF OPERATION

13. 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, or their national equivalent:

(a) Dedicated;

(b) System high; and

(c) Multi-level.

Chapter II

ADDITIONAL MARKINGS

14. 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.

DEFINITIONS

15. "DEDICATED" SECURITY MODE OF OPERATION shall mean: 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 with a common need-to-know for ALL of the information handled within the System.

Notes:

(1) The common need-to-know indicates there is no mandatory requirement for computer security features to provide separation of information within the System.

(2) Other security features (for example, physical, personnel and procedural) shall conform to the requirements for the highest classification level and all category designations of the information handled within the System.

16. "SYSTEM HIGH" SECURITY MODE OF OPERATION shall mean: 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.

Notes:

(1) The lack of common need-to-know indicates that there is a requirement for computer security features to provide selective access to, and separation of, information within the System.

(2) Other security features (for example, physical, personnel and procedural) shall conform to the requirements for the highest classification level and all category designations of the information handled within the System.

(3) All information handled or being available to a System under this mode of operation, together with output generated, shall be protected as potentially of the information category designation and of the highest classification level being handled until determined otherwise, unless there is an acceptable level of trust that can be placed in any labelling functionality present.

17. "MULTI-LEVEL" SECURITY MODE OF OPERATION shall mean: 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.

Notes:

(1) This mode of operation permits, currently, the handling of information of different classification levels and of mixed information category designations.

(2) The fact that not all individuals are cleared to the highest levels, associated with a lack of common need-to-know, indicates that there is a requirement for computer security features to provide elective access to, and separation of, information within the System.

18. INFORMATION SECURITY **(**INFOSEC**)** shall mean: the application of security measures to protect information processed, stored or transmitted in communication, information and other

electronic Systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the Systems themselves. INFOSEC measures include those of computer, transmission, emission and cryptographic security, and the detection, documentation and countering of threats to information and to the Systems.

19. COMPUTER SECURITY (COMPUSEC) shall mean: 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.
20. COMPUTER SECURITY PRODUCT shall mean: a generic computer security item which is intended for incorporation into an IT System for use in enhancing, or providing for, confidentiality, integrity or availability of information handled.
21. COMMUNICATIONS SECURITY (COMSEC) shall mean: 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 confidentiality or integrity of such telecommunications.

Note:

Such measures include cryptographic, transmission and emission security; and also include procedural, physical, personnel, document and computer security.

22. COMMUNICATIONS SECURITY PRODUCT shall mean: a generic communications security item which is intended for incorporation into a communications System for use in enhancing, or providing for, confidentiality, integrity or availability of information handled.
23. EVALUATION shall mean: the detailed technical examination, by an appropriate authority, of the security aspects of a System or of a communications or a computer security product.

Notes:

(1) The evaluation investigates the presence of required security functionality and the absence of compromising side effects from such functionality and assesses the incorruptibility of such functionality.

(2) The evaluation determines the extent to which the security requirements of a System, or the security claims of a computer security product, are satisfied and establishes the assurance level of the System or of the communications, or the computer security product's trusted function.

24. CERTIFICATION shall mean: a formal statement issued by an appropriate certification authority**,** supported by an independent review of the conduct and results of an evaluation, of the extent to which a System meets the security requirement, or a communications or computer security product meets pre-defined security claims.
25. APPROVAL of a cryptographic product for use shall mean: a formal statement issued by a National Approval Authority, following its own criteria, supported by the results of an evaluation. It is a necessary but not sufficient condition leading to accreditation.
26. ACCREDITATION shall mean: the authorisation of a System to process ESA classified information in its operational environment.

Note:

Such accreditation should be made after all appropriate security procedures have been implemented and a sufficient level of protection of the System resources has been achieved. Accreditation should normally be made on the basis of the SSRS, including the following:

(a) A statement of the objective of accreditation for the System; in particular, what classification level(s) of information are to be handled and what System or network security mode(s) of operation is being proposed;

(b) Production of a risk management review to identify the threats and vulnerabilities and measures to counter them;

(c) The Security Operating Procedures (SecOPs) with a detailed description of the proposed operations (e.g., modes, services, to be provided) and including a description of the System security features which shall form the basis of accreditation;

(d) The plan for the implementation and maintenance of the security features;

(e) The plan for initial and follow-on System security or network security test, evaluation, and certification; and

(f) Certification, where required, together with other elements of accreditation.

(g) For communications security products, a secondary evaluation may be required depending on the level of change to the approved version of the SSRS document.

27. IT SYSTEM shall mean: assembly of equipment, methods and procedures, and personnel, organised to accomplish information processing functions.

Notes:

(1) This is taken to mean an assembly of facilities, configured for handling information within the System.

(2) Such Systems may be in support of consultation, command, control, communications, scientific or administrative applications including word processing;

(3) The boundaries of a System will generally be determined as being the elements under the control of a single ITSOA/TSO.

(4) An IT System may contain subsystems some of which are themselves IT Systems.

28. IT SYSTEM SECURITY FEATURES comprise all hardware/ firmware/ software functions, characteristics, and features; operating procedures, accountability procedures, and access controls, the IT area, remote terminal/workstation area, and the management constraints, physical structure and devices, personnel and communications controls needed to provide an acceptable level of protection for classified information to be handled in an IT System.
29. IT NETWORK shall mean: organisation, geographically disseminated, of IT Systems interconnected to exchange data, and comprising the components of the interconnected IT Systems and their interface with the supporting data or communications networks.

Notes:

(1) An IT network can use the services of one or several communications networks interconnected to exchange data; several IT networks can use the services of a common communications network.

(2) An IT network is called "local" if it links several computers together on the same site.

30. IT NETWORK SECURITY FEATURES include the IT System security features of individual IT Systems comprising the network together with those additional components and features associated with the network as such (for example, network communications, security identification and labelling mechanisms and procedures, access controls, programs and audit trails) needed to provide an acceptable level of protection for classified information.
31. IT AREA shall mean: an area which contains one or more computers, their local peripheral and storage units, control units and dedicated network and communications equipment.

Note:

This does not include a separate area in which remote peripheral devices or terminals/workstations are located even though those devices are connected to equipment in the IT area.

32. REMOTE TERMINAL/WORKSTATION AREA shall mean: an area containing some computer equipment, its local peripheral devices or terminals/workstations and any associated communications equipment, separate from an IT area.
33. TEMPEST: security measures intended to protect equipment and infrastructures against the compromise of classified information through unintentional electromagnetic emissions.
34. TECHNICAL SYSTEMS OWNER (TSO) shall mean: the authority responsible for the creation, maintenance, operation and closing down of a System.

Chapter III

Security responsibilities

GENERALITIES

35. The responsibilities of the Security Committee, defined in Section I, paragraphs 3 and 4 include INFOSEC issues. The Security Committee shall organise its activities in such a way that it can provide expert advice on the above issues.
36. The ESA Security Office shall have an INFOSEC Unit, which shall be responsible, inter alia, for issuing detailed INFOSEC guidance, based on the provisions in this chapter.
37. In case of problems regarding security (incidents, breaches, etc.), immediate action shall be taken by the responsible National Authority and/or the ESA Security Office. All problems shall be communicated to the ESA Security Office, which shall be responsible for recording and

analysing the data and taking appropriate actions, pursuant to the provisions set out in Section X of these regulations. In the case of cryptographic violation or compromise, the provisions of chapter V of this Section on Communications Security shall apply.

SECURITY ACCREDITATION AUTHORITY (SAA)

38. The SAA shall be either:
    - an NSA or other competent authority, when the System handling ESA classified information is deployed under its national responsibility;
    - The Head of the ESA Security Office, for Systems not connected with a national information System and not using or processing national classified information;
    - A panel staffed by ESA and the appropriate NSAs, when different components of a System come under the jurisdiction of ESA and Member States.
39. The SAA shall be responsible for ensuring the compliance of Systems with the ESA security regulations. One of its tasks shall be to accredit a System to handle ESA classified information to a defined level of classification in its operational environment.
    - The jurisdiction of the ESA SAA shall cover all the Systems that are in operation within the premises of ESA (i.e. ESA headquarters, establishments and facilities).
    - Systems and components of Systems in operation within a Member State shall remain under the jurisdiction of that Member State.
    - When different components of a System come under the jurisdiction of the ESA SAA and others' SAAs, all the parties will appoint a joint accreditation panel under the coordination of the ESA SAA with the participation of representatives of the appropriate NSAs/DSAs.

INFOSEC AUTHORITY (IA)

40. The Head of the ESA Security Office INFOSEC Unit is the INFOSEC Authority for ESA. The ESA INFOSEC Authority is responsible for:
    - Implementing and operating security features of a System,
    - Auditing and controlling the correct application of the Security Regulations within ESA,
    - Providing technical advice and assistance to the SAA,
    - Assisting in the development of the SSRS,
    - Reviewing the SSRS to ensure consistency with these Security Regulations and the INFOSEC policies and architecture documents,
    - Issuing detailed INFOSEC guidance, based on the provisions in this chapter,
    - Participating in the accreditation panels/boards as required and providing INFOSEC recommendation on accreditation to the SAA,
    - Providing support to the INFOSEC training and education activities,
    - Providing technical advice in investigation of INFOSEC related incidents,
    - Establishing technical policy guidance to ensure that only authorised software is used.

IT SYSTEM OPERATIONAL AUTHORITY (ITSOA)/The Technical Systems Owner

41. The INFOSEC Authority 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 ITSOA or to the owner of that System, the Technical Systems Owner (TSO), as appropriate. This responsibility shall extend throughout the life cycle of the System from the project concept stage to final disposal.
42. The ITSOA/TSO shall be responsible for all security measures designed as part of the overall System. This responsibility includes the preparation of the SecOPs. The ITSOA/TSO shall specify the security standards and practices to be met by the supplier of the System.
43. The ITSOA/TSO may delegate a part of its responsibilities where appropriate to, the INFOSEC officer for a project or programme. The various INFOSEC functions may be performed by a single person.

USERS

44. All users shall be responsible for ensuring that their actions do not adversely affect the security of the System that they are using.

INFOSEC TRAINING

45. INFOSEC education and training shall be made available by the INFOSEC Authority at various levels, and for various personnel, as appropriate, within ESA Headquarters, establishments and facilities or national bodies.

Chapter IV

Non-technical security measures

PERSONNEL SECURITY

46. Users of the System shall be cleared and have a need-to-know, as appropriate for the classification and content of the information handled within their particular System. Access to certain equipment or information specific to security of Systems will call for special clearance issued according to specific existing national regulations.
47. The SAA shall designate all sensitive positions and specify the level of clearance and supervision required by all personnel occupying them taking account of the effects of aggregation where appropriate.
48. Systems shall be specified and designed in a way that facilitates the allocation of duties and responsibilities to personnel so as to prevent one person having complete knowledge or control of the System security keys points. The aim should be that collusion between two or more individuals would be necessary for alteration or intentional degradation of the System or network to take place.

PHYSICAL SECURITY

49. IT and remote terminal/workstation areas (as defined in paragraphs 31 and 32) in which information classified ESA CONFIDENTIAL and above is handled by IT means, 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 appropriate.
50. IT and remote terminal/workstation areas in which the security of the System can be modified shall not be occupied by only one authorised person.

CONTROL OF ACCESS TO A SYSTEM

51. 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.
52. 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 65 to 67.

Chapter V

Technical security measures

SECURITY OF INFORMATION

53. It shall be incumbent upon the originator of the information to identify and classify all information-bearing documents, whether they are in the form of hard-copy output or computer storage media. Each page of hard-copy output shall be marked, at the top and bottom, with the classification. Output, whether it is the form of hard-copy or computer storage media shall have the same classification as the highest classification of the information used for its production. The way in which a System is operated may also impact on the classification of outputs of that System.
54. ESA Directorates and their information holders 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.
55. When information is transferred from one System to another the information shall be protected during transfer and in the receiving System in the manner commensurate with the original classification and category of the information.
56. 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.

57. Reusable computer storage media used for recording ESA 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 65 to 67).

CONTROL AND ACCOUNTABILITY OF INFORMATION

58. Automatic (audit trails) or manual logs shall be kept as a record of access to information classified ESA SECRET and above. These records shall be retained in accordance with these security regulations.
59. ESA classified outputs held within the IT area may be handled as one classified item and need not be registered, provided the material is identified, marked with its classification and controlled in an appropriate manner.
60. Where output is generated from a System handling ESA classified information, and transmitted to a remote terminal/workstation area from an IT area, procedures, agreed by the SAA shall be established for controlling the remote output. For ESA SECRET and above, such procedures shall include specific instructions for accountability of the information.

HANDLING AND CONTROL OF REMOVABLE COMPUTER STORAGE MEDIA

61. All removable computer storage media classified ESA CONFIDENTIAL and above shall be handled as material and general rules will apply. Appropriate identification and classification markings need to be adapted to the specific physical appearances of the media, to enable it to be clearly recognised.
62. Physical removal of ESA classified information held in electronic form from ESA Headquarters, establishments and facilities, shall be in accordance with procedures approved by the SAA.
63. Users shall take the responsibility for ensuring that ESA classified information is stored on media with the appropriate classification marking and protection. Procedures shall be established to ensure that, for all levels of ESA information, the storage of information on computer storage media is being carried out in accordance with these security regulations.

DECLASSIFICATION AND DESTRUCTION OF COMPUTER STORAGE MEDIA

64. Computer storage media used for recording ESA classified information may be downgraded or declassified in accordance with a procedure to be approved by the SAA.
65. Computer storage media, which has held ESA SECRET and above information shall not be declassified and reused.
66. If computer storage media cannot be declassified or is not reusable, it shall be destroyed in accordance with the above procedure.

COMMUNICATIONS SECURITY

67. When ESA classified information is transmitted, special measures shall be implemented to protect the confidentiality, integrity and availability of such transmissions. The SAA shall determine the requirements for protecting transmissions based upon the requirements for confidentiality, integrity and availability.
68. Cryptographic products used to provide confidentiality, integrity or availability of ESA classified information shall have been evaluated and approved by an appropriately qualified authority of an ESA Member State.
69. During transmission, the confidentiality of information classified ESA SECRET and above shall be protected by cryptographic methods or products approved by the ESA Council upon recommendation of the ESA Security Committee. During transmission, the confidentiality of information classified ESA CONFIDENTIAL or ESA RESTRICTED shall be protected by cryptographic methods or products approved either by the Director General upon recommendation of the ESA Security Committee or approved by a Member State's NSA/DSA.
70. Detailed rules applicable to the transmission of ESA classified information shall be set out in specific security instructions approved by the Director General upon recommendation of the ESA Security Committee.
71. Under exceptional operational circumstances, information classified ESA RESTRICTED, ESA CONFIDENTIAL and ESA SECRET may be transmitted 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 means of encryption are not available, and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations.

72. A System shall have the capability of positively denying access to ESA classified information at any or all of its remote workstations or terminals, when required either by physical disconnection or by special software features approved by the SAA.

INSTALLATION AND RADIATION SECURITY

73. Initial installation of Systems and any major change thereto shall be so specified that installation is carried out by security cleared installers under constant supervision by technically qualified personnel who are cleared for access to ESA classified information to the level equivalent to the highest classification which the System is expected to store and handle.
74. All equipment shall be installed in accordance with the current ESA Council's Security Regulations.
75. 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".
76. TEMPEST measures for ESA Headquarters, establishments and facilities shall be reviewed and approved by the Head of the ESA Security Office acting as TEMPEST authority.

Chapter VI

Security during handling

SECURITY OPERATING PROCEDURES (SecOPs)

77. SecOPs define the principles to be adopted on security matters, the operating procedures to be followed, and personnel responsibilities. The SecOPs shall be prepared under the responsibility of the ITSOA/TSO.

SOFTWARE PROTECTION/CONFIGURATION MANAGEMENT

78. Security protection of applications programmes shall be determined on the basis of an assessment of the security classification of the programme itself rather than of the classification of the information it is to process. The software versions in use should be verified at regular intervals to ensure their integrity and correct functioning.
79. New or modified versions of software should not be used for the handling of ESA classified information until verified by the ITSOA/TSO.

CHECKING FOR THE PRESENCE OF MALICIOUS SOFTWARE/COMPUTER VIRUSES

80. Checking for the presence of malicious software/computer viruses shall be periodically carried out in accordance with the requirements of the SAA.
81. All computer storage media arriving in ESA headquarters, establishments or facilities shall be checked for the presence of any malicious software or computer viruses, before being introduced to any System using tools and facilities approved by the ESA Security Office.

MAINTENANCE

82. 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 entering to an IT area.
83. 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.

Chapter VII

ACCREDITATION

84. All Systems for which a SSRS has to be produced, prior to handling ESA classified information, shall be accredited, based upon information provided in the SSRS, SecOPs and any other relevant documentation, by the SAA. Subsystems and remote terminals/workstations shall be accredited as part of all the Systems to which they are connected. Where a System supports both ESA and other organisations, ESA and the relevant Security Authorities shall mutually agree on the accreditation.

85. The accreditation process may be carried out in accordance with an accreditation strategy appropriate to the particular System and defined by the SAA.

EVALUATION AND CERTIFICATION

86. Any security product (except cryptographic products) to be used with the System to be procured shall either have been evaluated and certified, or currently be under evaluation and certification by an appropriate Evaluation or Certification body of one of the ESA Member States against internationally acknowledged criteria (such as the Common Criteria for Information Technology Security Evaluation, see ISO 15 408).
87. Prior to accreditation, in certain instances, the hardware, firmware and software security features of a System shall be evaluated and certified as being capable of safeguarding information at the intended level of classification.
88. The requirements for evaluation and certification shall be included in System planning, and clearly stated in the SSRS.
89. Where appropriate, technically qualified and appropriately cleared personnel acting on behalf of the ITSOA/TSO will ensure the use of certified products. The personnel may be provided from a nominated Member State's evaluation or certification authority or its nominated representatives, for example a competent and cleared contractor.

Note: for cryptographic products see paragraph 69.

90. The degree of evaluation and certification processes involved may be lessened (for example, only involving integration aspects) where Systems are based on existing nationally evaluated and certified computer security products.

ROUTINE CHECKING OF SECURITY FEATURES FOR CONTINUED ACCREDITATION

91. The ITSOA/TSO shall establish routine control procedures, which shall ensure that all security features of the System are still valid.
92. 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/TSO 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.
93. 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.

Chapter VIII

Temporary or occasional use

SECURITY OF MICROCOMPUTERS/PERSONAL COMPUTERS

94. Microcomputers/Personal Computers (PCs) with fixed disks (or other non-volatile storage media), operating either in stand-alone mode or as networked configurations, and portable computing devices (for example, portable PCs and electronic "notebooks") with fixed hard disks, shall be considered as information storage media in the same sense as floppy diskettes or other removable computer storage media.
95. 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 (until downgraded or declassified in accordance with approved procedures).

USE OF PRIVATELY-OWNED IT EQUIPMENT FOR OFFICIAL COUNCIL WORK

96. The use of privately-owned removable computer storage media, software and IT hardware (for example, PCs and portable computing devices) with storage capability shall be prohibited for handling ESA classified information.
97. Privately-owned hardware, software and media shall not be brought into any Class I or Class II area where ESA classified information is handled without the permission of the Head of the ESA Security Office. This authorisation can only be provided for technical reasons in exceptional cases.

USE OF THE CONTRACTOR-OWNED OR NATIONALLY-SUPPLIED IT EQUIPMENT FOR OFFICIAL COUNCIL WORK

98. The use of contractor-owned IT equipment and software in organisations in support of official ESA Council work may be permitted by the Head of the ESA Security Office. The use of nationally-provided IT equipment and software may also be permitted; in this case, the IT equipment shall be brought under the control of the appropriate ESA's inventory. In either case, if the IT equipment is to be used for handling ESA classified information, then the SAA shall be consulted in order that the elements of INFOSEC that are applicable to the use of that equipment are properly considered and implemented.

SECTION XII

RELEASE OF ESA CLASSIFIED INFORMATION TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

PRINCIPLES REGULATING THE RELEASE OF ESA CLASSIFIED INFORMATION

1. The release of ESA classified information to third States or international organisations will be decided by the ESA Council on the basis of:
   - The nature and content of such information,
   - The recipients' need to know,
   - The measure of advantages to ESA.

   The Member State originator of the ESA classified information to be released will be asked for its agreement. ESA classified information which was originated by an ESA Member State shall only be released with the approval of the originator, or, if the originator can no longer be identified, with the approval of the appropriate ESA Board or Committee.
2. These decisions will be taken on a case-by-case basis, depending on:
   - The desired degree of cooperation with the third States or international organisations concerned,
   - The confidence that may be placed in them, which ensues from the level of security that would be applied to the ESA classified information entrusted to those States or organisations and from the consistency between the security rules applicable there and those applied in ESA. The ESA Security Committee will give the Council its technical opinion on this point.
3. Draft agreements on security procedures or memoranda of understanding will be approved by the Security Committee before they are presented to the Council for a decision.

SECTION XIII

INDUSTRIAL SECURITY

General principles

1. This title deals with security aspects of industrial activities that are unique to the negotiation and placing of ESA classified contracts (i.e. contracts involving classified information pursuant to the ESA Security Agreement) and their performance by industrial entities, including the release of ESA classified information during the bidding period and pre-contract negotiations.
2. All entities participating in industrial activities, which involve access to ESA information classified ESA CONFIDENTIAL and/or ESA SECRET must hold a Facility Security Clearance (FSC). An FSC is granted by a NSA/DSA to confirm that, from a security viewpoint, a facility can afford and guarantee 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.
3. ESA, in co-operation with its Member States, will determine, as appropriate, the aspects of an ESA programme or element of a programme requiring security protection. The ESA Security Committee and the appropriate ESA Subordinate Body will recommend the security classification to be accorded to each aspect area of the programme to ESA Council for approval.
4. Prior to the release of information classified ESA CONFIDENTIAL and/or ESA SECRET to a contractor, potential contractor, or sub-contractor, the NSA/DSA will:
   a. ensure that such contractor(s), potential contractor(s), or sub-contractor(s) and their facility(ies) have the capability to protect the information adequately;

b. grant Facility Security Clearances (FSC) to the facility(ies);
c. grant Personnel Security Clearances (PSC) to all persons whose duties require access to ESA information classified CONFIDENTIAL and/or SECRET;
d. ensure that access to ESA classified information is limited to those persons who have a need-to-know for the purpose of performing ESA activities;
e. upon request of the ESA Security Office or any Member State, grant a FSC to enable an entity to bid for, negotiate or perform an ESA classified contract, sub-contract;
f. provide, upon request, to the ESA Security Office or any Member State, a PSC assurance for persons having security responsibilities to enable them to perform on an ESA classified contract which may also include international visits;
g. take action with regard to the specific arrangements to be carried out in matters of transportation in accordance with paragraphs 26 to 40 of this Section;
h. to ensure that, for any entity in which ESA classified information is to be used, security officials are appointed to effectively exercise the responsibilities for safeguarding ESA classified information. These officials will be responsible for limiting access to ESA classified information involved in a contract to those persons who have been appropriately security cleared for access and have a need-to-know.

5. The competent authorities of the Member States will investigate all cases in which it is known or where there are grounds for suspecting that ESA classified information provided or generated pursuant to an ESA contract has been lost, compromised or disclosed to unauthorised persons. Each NSA/DSA will comply with the investigative requirements in Section X of these regulations.

Security requirements for ESA classified contracts

6. The programme implementing rules approved by ESA Council shall contain a Programme Security Instruction (PSI) with security standards no less stringent than the provisions set out in this section.
7. The PSI shall be annexed to the Prime contract. A „Programme Security Classification Guide“ shall be a part of the PSI. All ESA classified subcontracts shall include the Programme Security Classification Guide or, as a minimum, a “Security Aspect Letter” (SAL) which sets out the classified aspects of a subcontract. The PSI and/or SAL shall be the single source document for the security of the contract. Such security rules will meet with ESA Security Regulations outlined in this document and comply with the respective national laws and regulations of the Member States where the contract is placed.
8. All contracts shall contain the “ESA security clauses for classified contracts” as approved by the ESA competent bodies.
9. In respect of all contracts classified ESA CONFIDENTIAL and/or ESA SECRET, the prime contractor shall notify the NSA/DSA of the Member State in which the entity that has been awarded the contract is located or incorporated, that a classification guide or a Security Aspect Letter (SAL) has been provided to that entity together with the contract.
10. The classification for elements of information associated with possible subcontracts shall be based on the Program Security Classification Guide.
11. The prime contractor and subsequent subcontractors shall be contractually bound, under penalty of termination of their contract, to take all measures prescribed by ESA and/or NSAs/DSAs respectively for safeguarding all ESA classified information generated by or entrusted to the contractor, or embodied in articles manufactured by the contractor.
12. The obligation of these Security Regulations including the confidentiality of the classified information shall continue to be observed by the contractors and subsequent subcontractors after termination or conclusion of an ESA classified contract or subcontract.

Placing of ESA classified contracts involving ESA information classified CONFIDENTIAL or SECRET

13. ESA classified contracts will be placed according to the policies established by ESA.
14. The prime contractor, if duly authorised by ESA, may negotiate subcontracts with other contractors, i.e., subcontractors. The prime contractor will be responsible for all subcontracting activities.
15. The following general principles will be observed in connection with the security classification requirements of ESA classified contracts:

a) the determination of classification levels is the responsibility of the originator of the information;
b) classifications should apply only to those aspects of a contract that must effectively be protected and such classifications should be strictly related to the degree of protection required;
c) a compilation of information from more than one source will require co-ordination of the sources in the determination of the appropriate ESA classification level;
d) provisions should be made for the downgrading and declassification as soon as it is possible;
e) changes in the level of classification should be made only with the prior consent of the originator.

16. The initial assessment of a level of classification of a contract where components are not defined and which involve the development of systems rests with the contractor.
17. The levels of classification for possible sub-contracts will be based on the Programme Security Instruction or the Security Aspect Letter of the contracts to which they are related.
18. Before a potential contractor is authorised to negotiate an ESA classified contract involving information classified CONFIDENTIAL and/or SECRET, the ESA Security Office will request the NSA/DSA of this potential contractor for confirmation that it holds an appropriate or provisional FSC, in compliance with national rules and regulations, at least equal to the classification level of the information that will be required for the negotiation of the contract. The NSA/DSA will provide confirmation or otherwise that the potential contractor or sub-contractor holds an FSC or a provisional FSC, in compliance with national rules and regulations. If the potential contractor has no FSC or the FSC is not at the required level, the ESA Security Office shall forward a request to the NSA/DSA for the initiation/upgrading of a FSC using the “Facility security clearance information sheet”(FIS) at Annex 3.
19. All invitations to bid in respect of ESA classified contracts will contain a clause requiring a potential contractor who does not submit a bid to return all documents which were provided to enable him to submit a bid to the contracting officer by the date set for the opening of bids. Similarly, an unsuccessful bidder will be required to return all documents after a stipulated period of time (normally within 15 days after notification that a bid or negotiation proposal was not accepted).
20. At whatever level it is proposed to bid for or to negotiate a sub-contract, the following will apply:
    a) before entering into negotiations, the Security Officer of the contractor will request its NSA/DSA for confirmation that the potential subcontractor holds an appropriate FSC ;
    b) when the potential sub-contractor is under the jurisdiction of another NSA/DSA, the NSA/DSA of the contractor will issue the request to the former;
    c) NSA/DSA of the potential sub-contractor will return the completed form together with the required information to the contractor, following the same channels;
    d) 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 ESA classified information issued to the latter.
21. All contractors shall, for contracts classified ESA CONFIDENTIAL and/or SECRET, always hold an FSC and shall ensure that their representatives involved in the negotiations hold an appropriate Personal Security Clearance (PSC), issued in accordance with Section V above, and only receive access to ESA classified information needed for the negotiation of the contract. For contracts classified ESA RESTRICTED, a FSC or PSC is not required unless specifically required by national security rules and regulations.
22. Conditions to bid for and negotiate a contract by a potential contractor or subcontractor not considered to belong to an ESA Member State (Article II.3 Annex V of ESA Convention) or located in a non-ESA Member State shall be provided for in the implementing rules of the programme.

Industrial Security Clearances for ESA contracts

23. A contractor may bid on, participate in pre-contractual negotiations or perform on a ESA contract classified ESA CONFIDENTIAL and/or SECRET, provided the NSA/DSA of the Member State in which the contractor is located and incorporated to do business has given the contractor’s entity the requisite level of FSC or provisional FSC, and all persons who may have access to

classified information have been issued the requisite level of PSC in accordance with the Section V of this document. Contractors in possession of a provisional FSC will need to be granted a full FSC upon award of a ESA Contract classified CONFIDENTIAL and/ or SECRET**.**

24. Applications for the security clearance for persons working for contractor entities shall be made to the NSA/DSA, which is responsible for the entity.
25. If an entity wishes to employ a national of a non-ESA Member State in a position that requires access to ESA 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 prescribe herein, and determine that the individual can be granted access in accordance with Section V.

Transmission of documents/material classified ESA CONFIDENTIAL or ESA SECRET between Member States.

26. Information classified ESA CONFIDENTIAL and/or ESA SECRET will normally be transferred between ESA and its Member States through government-to-government diplomatic channels or through channels approved by the NSAs/DSAs of the Member States.

International transportation of ESA classified material

27. The following principles shall be enforced when examining proposed security arrangements for the international transportation of consignments of classified material:
    (a) security shall be assured at all stages during the transportation and under all circumstances, from the point of origin to the ultimate destination;
    (b) the degree of protection accorded to a consignment shall be determined by the highest classification level of material contained within it;
    (c) an FSC shall be obtained, where appropriate, for entities providing transportation. In such cases, personnel handling the consignment shall be cleared according to an appropriate level;
    (d) journeys shall be point-to-point to the extent possible, and shall be completed as quickly as circumstances permit, and
    (e) care shall be exercised to arrange routes only through ESA Member States. Routes through non ESA Member States should only be undertaken when authorised by the NSA/DSA of the consignors Member State and the consignee.
28. Arrangements for consignments of classified material shall be stipulated between the NSA/DSA concerned. However, such arrangements shall ensure that there is no likelihood of unauthorised access to classified material.

Packaging of Documents and small-sized material

29. Packaging of consignments shall be in compliance with Section VII of these regulations. The Security Officer of the consignor facility is responsible for the supervision of packaging. Special cases requiring additional guidance should be discussed with the facility's NSA/DSA. In no circumstances shall the packaging reveal the fact that the material is classified.

Hand carriage of ESA classified documents/material

30. When transmission through channels specified in Section VII will result in an unacceptable delay that will adversely affect performance of the ESA contract and when it has been verified that the information is not available at the intended destination, the procedures of hand carriage may be permitted provided the following provisions are complied with:
    a) the courier shall be a permanent staff or employee of the dispatching or receiving entity. Shipping agents or commercial courier services shall not be used;
    b) the procedure shall be used on a case-by-case basis, subject to the prior approval by the NSAs/DSAs of the Member States concerned.
    c) the courier holds the appropriate security clearance;
    d) the courier is aware of his responsibilities for safe custody; the courier must carry a courier certificate or a multi-travel courier certificate authorising him to carry the package as identified as well as a copy of "Notes for the courier" (see Annex 1 and appendices for ESA staff members and experts and Annexe 2 and appendices for any other person); a record of the documents/material so carried is held in the appropriate office or registry of the dispatching facility.
31. The dispatching authority/facility will notify the receiving authority/facility about the details (e.g. time of arrival, name of courier) prior to the hand-carriage taking place.

32. Under no circumstances shall the classified consignment be handed over to Customs or other public officials for their custody.

Transportation of items classified ESA CONFIDENTIAL and/or ESA SECRET by Commercial Carriers as Freight

33. 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:
    a) hold an appropriate FSC issued by the NSA/DSA of the ESA Member State of origin if deemed necessary and according to national security regulations;
    b) be authorised by laws or regulations of the ESA Member State of origin to provide international transportation services;
    c) is obligated to comply with safety, security and emergency procedures which must be observed.

Transportation by road

34. The following standards shall be applied when consignments of ESA classified material are transmitted by road transportation:
    a) if required by national rules and regulations, 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 secured in vehicles or containers by a lock or padlock, closed van or cars that may be sealed;
    c) containers must bear no visible indication of their contents;
    d) consignments will be transported point-to-point;
    e) the consignor and the consignee are responsible for jointly organising the transport and for its notification to their respective NSA/DSA who should jointly approve the transportation plan;
    f) where appropriate the NSAs/DSAs will advise their customs or other relevant national authorities of impending consignments and should be urged to give maximum priority to the shipment.
35. If the classified consignment cannot be secured as described in paragraph 34.b) the consignment should be encased or sheathed so as to protect the classified aspects and prevent unauthorised persons from gaining access.

Transportation by rail

36. Transportation by rail may be used for consignments of ESA classified material on the basis of the following condition: passenger accommodations shall be made available for security guard personnel and during stops the security guard shall remain with the consignment.

Transportation by sea

37. The following standards shall be applied when consignments of ESA material classified CONFIDENTIAL and/or SECRET are sent by sea:
    a) a cleared guard or escort shall accompany the consignment;
    b) material shall be stowed in locked stowage space approved by the NSA/DSA of the consignor. The consignment must be under security control;
    c) stops at maritime countries presenting special security risks shall be assessed by the NSAs/DSAs of the consignor/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 concerned;
    d) stops at any non ESA member States' port shall not be permitted unless prior approval of the consignor's NSA/DSA has been obtained;
    e) in all cases, loading and unloading shall be under security control;
    f) deliveries 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

38. An air carrier may be used provided the following standards shall be applied:
    a) Airlines of ESA Member States shall normally be used. However in exceptional circumstances such as the extreme size of the consignment, airlines of non ESA Member States may be used in consultation with the NSA/DSA of the consignor;

b) the consignment shall be delivered straight to the aircraft rather than being stored in warehouses, etc.. at airports, airfields. A sufficient number of security guards must be provided to keep the consignment under adequate supervision;

c) every effort shall be made for the aircraft to be met on landing and the consignment to be removed at its final destination.

d) Intermediate routine stops of short duration may be permitted, provided the consignment shall remain in the aircraft;

e) In the event the aircraft is delayed at an intermediate stop or has to make an emergency landing, the security guard shall take all measures considered necessary for the protection of the consignment;

f) Direct flights shall be used whenever possible and, except in an emergency, stops at airfields in non ESA Member State shall not be permitted unless final destination is in a non ESA Member State.

Security Guards and Escorts

39. Individuals fulfilling the duties of security guards may be armed or unarmed depending on national practices and arrangements made by between the NSAs/DSAs of the Member States affected by the transportation. They must be nationals of ESA Member States and be security cleared.

40. The security guard/escort shall be composed of an adequate number of personnel as to ensure 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.

41. It is the responsibility of the consignor and, where applicable, the consignee to instruct security guards in their duties. Security guards shall also be given a copy of “Notes for the Courier” (appendix 2 to Annex 1) and be required to sign a receipt for it.

Transportation of items classified ESA RESTRICTED

42. ESA RESTRICTED items will be transported in accordance with the provisions set out in paragraph 21 of Section VII.

International visits

43. International visits involving access to information classified ESA CONFIDENTIAL and ESA SECRET will be subject to approval, in accordance with the rules and regulations of the receiving Member State. The procedures for ESA international visits are based on the use of the “Request for visit” (RFV) as shown at Annex 4.

44. ESA, national bodies, contractors and subcontractors, which intend to send personnel on international visits, shall submit to the NSA/DSA of the entity to be visited, through the agreed official channels, an international visit request in accordance with the procedures set out in the PSI and/or SAL. The visit request shall include an assurance/certification of Personnel Security Clearance for each visitor.

45. The procedures apply to the following types of visits:

a) one-time visits – single visits for a specified purpose, normally lasting less than 15 days and which are not anticipated to be repeated within the year;

b) recurring visits –intermittent, recurring visits over a specified period of time, normally not exceeding one year and for a special purpose; and

c) emergency visits – one-time visits that must take place as a matter of urgency and importance, such that the standard visit request procedure cannot be used.

46. Request for recurring visits should normally be used for contracts for all ESA programmes. They shall be valid for one year from the start date requested in the RFV. Recurring visits shall be re-submitted for the re-issuance annually.

47. To qualify as an emergency visit, the following conditions shall be met:

a) the proposed visit is related to an official ESA request for proposal/request for tender offer, or

b) the visit is to be made in response to the invitation of the host national body or the ESA Programme Management Office; or

c) a ESA programme will be adversely affected if the visit request is not approved.

48. Where permitted by national security rules and regulations, ESA RESTRICTED visits may be arranged directly between the Security Office for the visitor and the Security Office of the entity to be visited.

49. The ESA international visit procedures will normally be those defined in Annex 4. However, in case of a specific programme, when all NSAs/DSAs involved determine that these general procedures would not be the best suitable for their specific requirements, they may establish more flexible procedures, in coordination with the ESA Security Office, provided that these are compatible with the principles set out in this section and allow such authorities to obtain the same information and the same essential guarantees of security. The ESA international visit procedures will then be those defined in Annex 5.

Annex 1

EUROPEAN SPACE AGENCY

…….

(programme title)

COURIER CERTIFICATE

COURIER CERTIFICATE N°_____

For the international hand carriage of classified documents, equipment and/or components classified ESA CONFIDENTIAL or ESA SECRET

This is to certify that the bearer,

Mr./Mrs/Miss: (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: _____

is authorised to carry on the journey detailed below the following consignment: (number and particulars of the consignment)

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 treatments 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:

- the consignment will not be inspected without permission of a duly authorised representative of ESA nor retained.
- Customs, police and/or immigration officials of countries to be transmitted, entered or exited are requested to give assistance if necessary to ensure successful and secure delivery of the consignment.

(Name and signature of issuing security responsible).

Annex 1, Appendix 1

To courier certificate n°……

ITINERARY

From:	(originating country)
To:	(destination country)
Through:	(list intervening countries)
Authorised stops::	(list locations)
Date of beginning of journey	(day/month/year)

Signature of ESA Security Office

_____

(name)

ESA stamp

_____

N O T E: to be signed on completion of journey:

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

Courier's signature: _____

Witnessed by: Head of ESA Security Office's signature

Date of return of the "Courier Certificate": …… (day/month/year)

Annex 1, Appendix 2

To ESA courrier certificate n°….

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 understand 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 in your personal possession, unless you are accompanying a classified consignment under approved transportation plan.
3. The consignment will not be opened en route except in the circumstances described in paragraph 10 below.
4. The classified consignment is not to be discussed or disclosed in any public place.
5. The classified consignment must not, under any circumstances, be left unattended. During overnight stops, governmental facilities or industrial entities having appropriate security clearance may be utilised. You are to be instructed on this matter by your responsible Security officer.
6. While hand carrying or accompanying a classified consignment, you are forbidden to deviate from the travel schedule provided.
7. In cases 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 listed in paragraph 12 below.

If you have not received these details, ask for them from our responsible Security Officer.

8. You and the 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 other than the designated representatives of the entity or government you are to visit, you will give it only to authorised employees of one of the points of contacts listed in paragraph 12.
10. There should be 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 actual senior Customs, Police, and/or Immigration Official; this action should normally suffice to pass the consignment through unopened. However, if the senior Customs, Police, and/or Immigration Official demands to see the actual contents of the consignment you should contact the ESA Security Office.
11. If the customs authorities open the consignment, you should request them to reseal it and endorse the shipping documents confirming that the consignment was opened by such authorities.
12. Upon your return, you must produce a bona fide receipt for the consignment signed by the Security Officer of the entity or national body receiving the consignment or by an ESA Programme Direction.
13. Along the route you may contact the following officials to request assistance:

Annex 2

(INSERT NAME AND ADDRESS OF DSA)
PROGRAMME TITLE (optional)

COURIER CERTIFICATE NO._____

FOR THE INTERNATIONAL HAND CARRIAGE OF CLASSIFIED DOCUMENTS, EQUIPMENT AND/OR COMPONENTS

This is to certify that the bearer, Mr./Mrs/Miss: (name/title)
born on: (day/month/year), in (country),
a national of: (country),
holder of passport/identity card no: (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)

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

- The material comprising this consignment is classified in the interests of national 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 crossed also may be indicated.)
- It is requested that the consignment will not be inspected by other than properly authorised 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 reclosing 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 transmitted, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.

Annex 2, Appendix 1

To courier certificate No:.....

ITINERARY

From:	(originating country)
To:	(destination country)
Through:	(list intervening countries)
Authorised stops::	(list locations)
Date of beginning of journey	(day/month/year)

Signature of company's Security Officer	Signature of the Designated Security Authority, Cognisant Security Office or Designated Government Representative
(name)	(name)
Company's stamp	Designated Security Authority's stamp

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

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

Courier's Signature:

Witnessed by: (company Security Officer's signature)

Date of return of the „Courier Certificate“: (day/month/year)

Annex 2, Appendix 2

(Insert name and address of DSA)

DECLARATION

(Name, Forename) ……..

(Name of company) ……

(Position in company)……..……

…….

The Security Officer of

(name of company / organisation)

handed to me the Notes concerning the handling and custody of classified documents/equipment to be carried. I have read and understood their contents.

I shall always retain en route the classified documents/equipment and shall not open any package unless required by the Custom Authorities.

Upon each arrival, I shall hand over the classified documents/equipment intended for the receiving company/organisation, against receipt, to the designated consignee.

…… ……

(place and date) Signature of courier

Witnessed by……..……..

(company Security Officer's signature)

Annex 2, Appendix 3

(NAME AND ADDRESS OF DSA)

Appendix 2 to the „Courier Certificate“ for the International Hand Carriage of Classified Documents, Equipment, and/or Components

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 understand 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 in your personal possession, unless you are accompanying a classified consignment under NSA/DSA approved transportation plan.
3. The consignment will not be opened en route except in the circumstances described in 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 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 travel schedule provided.
7. In cases 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 listed in paragraph 12 below.
   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 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 paragraph 12.
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 actual senior Customs, Police and/or Immigration Official; this action should normally suffice to pass the consignment through unopened. However, if the senior Customs, Police, and/or Immigration Official demands to see the actual contents of the consignment you may open it in his presence, but this should be done in an area out of sight of the general public.

Annex 2, Appendix 3

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.
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 and signing them when closed and confirming in the shipping documents (if any) that the consignment has been opened.
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 NSAs/DSAs of their respective governments.

11. 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 NSA/DSA of the receiving government.
12. Along the route you may contact the following officials to request assistance:

.....
.....
.....
.....

Annex 2, Appendix 4

(Insert name and address of DSA)

Programme Title

MULTI-TRAVELS COURIER CERTIFICATE N° …….

for international hand carriage of classified DOCUMENTS, EQUIPMENTS AND/OR COMPONENTS

This is to certify that the bearer Mr/Mrs/Miss (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 with (company or organisation) : ……..……... is authorised to carry classified documents, equipments and/or components between the following countries :

……..……..……

The bearer above is authorised to use the present certificate as many times as necessary, for classified shipments between the countries here above until (date) : …….

Each sending is attached with the shipment description.

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 authorised 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 reclosing 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 transmitted, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.

Signature of company's Security Officer

Signature of the Designated Security authority, Cognisant Security Office or Designated Government representative

Annex 2, Appendix 4.1

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

(Insert name and address of DSA)

Note for the international multi-travels hand carriage of classified Documents, Equipment, and/ or Components

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 understand 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 open 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 paragraph 11 below. 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 inquire 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 actual senior Customs, Police, and/or Immigration Official; This action should normally suffice to pass the consignment through unopened. However, if the senior Customs, Police, and/or Immigration Official demands 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.

Annex 2, Appendix 4.1

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 routes you may contact the officials that will be provided to you before each travel and request assistance from them.
15. Upon each 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 NSA/DSA of the receiving government.

Annex 2, Appendix 4.2

To multi-travels courier certificate

No:.....

Description of shipment nr : ……..

Transport from (date) : …… to (date) : ……

Bearer (name) : ……

Itinerary : from (originating country) …… to (destination country) …… through (crossed countries) …… authorised stops (list of locations) : …….....

References of receipt or inventory list : ……

Description of the shipment (number of package, dimensions and, if needed, 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 3

EUROPEAN SPACE AGENCY

FSC 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 … as provided □□ □□ □□ (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 and Fax Number of Security Officer: ……	
6.	This request is made for the following reason(s): (indicate particulars of the precontractual stage, contract, sub-contract programme) ……. …….	
	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)
	In case of an earlier invalidation or in case of any information listed above, you will be informed		
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 NSA/DSA:	Name: Date:	

Annex 4

EUROPEAN SPACE AGENCY
REQUEST FOR VISIT *

1. □ One-time Date:
   □ Recurring Visit ID:
   □ Emergency
2. **Requesting Government / Agency or Industrial Facility:**

   Name:
   Postal address:
   Requesting Government / Agency or Industrial Facility:

3. Name:
   Address:

   Fax Nr.: telephone Nr.:
   Point of contact:
4. Dates of visit: to to
5. □ Government Initiative
   □ Commercial Initiative
   □ Initiated by requesting Agency or facility
   □ By invitation of the facility to be visited
6. Subject to be discussed/justification:

7. Anticipated level of classified information to be involved:
   Specify:
8. □ A specific equipment or weapon system
   □ Foreign military sales or export license
   □ A programme or agreement
   □ A defense acquisition process
   □ Other

* To be completed in the English language

Annex 4

Visit ID Number:

9. Particulars of Visitors
   Name:
   Date of Birth Place of Birth:
   Security Clearance ID/PP number:
   Position:
   Company/Agency:

   Name:
   Date of Birth Place of Birth:
   Security Clearance ID/PP number:
   Position:
   Company/Agency:
10. The Security Officer of the requesting government agency or industrial facility
11. Certification of Security Clearance
    Name: Stamp
    Address: (Optional)
    Telephone:

    Signature:

12. Requesting National Security Authority
    Name:
    Address: Stamp
    Telephone: (Optional)
    Signature:
13. Remarks

ESA/C/R/CLXI/Rules 1 (Final)

EUROPEAN SPACE AGENCY
REQUEST FOR VISIT *

□ One-time
□ Recurring
□ More than 21 days

REQUESTING ESTABLISHMENT / COMPANY / AGENCY:

Name: ……
Address: ……
Security Officer: ……
Telephone/Fax/E-mail: …… Point of contact: ……

DATE OF VISIT:

From: …….. To: ……..

SUBJECT TO BE DISCUSSED:

Project / Contract / Programme: ……

Anticipated Level of Discussions □ C □ S

VISITOR DETAILS:

Name: …… Passport n°: ……..
Date of Birth:……. Nationality: ……...…
Security Clearance Level: …… Expiry Date: ……
Rank / Grade: ..…
Company / Agency: …….. Position:

…….……

(Continue on additional sheets for extra visitors)

Signature: ……. Date: ……

* To be completed in the English language

Anlage 2 Teil I der Erläuterungen

SICHERHEITSVORSCHRIFTEN DER ESA – TEIL I

GRUNDPRINZIPIEN UND MINDESTNORMEN FÜR DEN SCHUTZ DER IM ZUSAMMENHANG MIT DEN TÄTIGKEITEN DER ESA HERVORGEBRACHTEN UND WEITERGEGEBENEN VERSCHLUSSSACHEN

EINLEITUNG

1. Die vorliegenden Bestimmungen enthalten die Grundprinzipien und Mindestnormen für die Sicherheit, die von der Europäischen Weltraumorganisation (im folgenden „die ESA“ genannt) und ihren Mitgliedstaaten anzuwenden sind, damit ESA-Verschlußsachen vor dem Verlust ihrer Vertraulichkeit, Integrität und Verfügbarkeit bewahrt bleiben. Im Einklang mit diesen Grundprinzipien und Normen werden in der ESA und ihren Mitgliedstaaten Sicherheitsprogramme eingeführt, die gemäß Artikel 3 des Sicherheitsübereinkommens der ESA einen Schutz in einheitlichem Umfang sicherstellen.
2. Die Hauptziele der ESA im Bereich der Sicherheit sind:
   a) Schutz von ESA-Verschlußsachen vor Spionage, Kenntnisnahme durch Unbefugte oder unerlaubter Weitergabe;
   b) Schutz von ESA-Verschlußsachen, die in Kommunikations- und Informationssystemen und -netzen behandelt werden, vor Gefahren für ihre Integrität und Verfügbarkeit;
   c) Schutz von Einrichtungen, in denen ESA-Verschlußsachen aufbewahrt werden, vor Sabotage und vorsätzlicher Beschädigung;
   d) im Falle des Versagens der Sicherheitsvorkehrungen Bewertung des entstandenen Schadens, Begrenzung seiner Folgen und Durchführung der erforderlichen Maßnahmen zu seiner Behebung.
3. Die Grundlagen für die Schaffung einer soliden Sicherheitslage sind:
   a) in jedem Mitgliedstaat eine nationale Sicherheitsbehörde (NSA)/benannte Sicherheitsbehörde (DSA), die sich zu vergewissern hat, daß in bezug auf alle Inländer, die Zugang zu als „ESA VERTRAULICH“ und höher eingestuften Informationen haben müssen, ein Sicherheitsunbedenklichkeitsbescheid ergangen ist;
   b) in jedem Mitgliedstaat eine nationale Sicherheitsstruktur, die dafür zuständig ist,
      i) Erkenntnisse über Spionage, Sabotage, Terrorismus und andere subversive Tätigkeiten zu sammeln und zu speichern sowie
      ii) ihre jeweilige Regierung und – über sie – den ESA-Rat über Art und Umfang von Bedrohungen der Sicherheit und entsprechende Schutzmaßnahmen zu informieren und zu beraten;
   c) in jedem Mitgliedstaat und in der ESA eine technische INFOSEC-Stelle, die dafür zuständig ist, in Zusammenarbeit mit der betreffenden Sicherheitsbehörde Informationen und Beratung über technische Bedrohungen der Sicherheit und entsprechende Schutzmaßnahmen bereitzustellen;
   d) eine regelmäßige Zusammenarbeit zwischen Regierungsstellen, Einrichtungen und den entsprechenden ESA-Dienststellen, um erforderlichenfalls
      i) die schutzbedürftigen Informationen, Ressourcen und Einrichtungen und
      ii) gemeinsame Schutznormen

   zu bestimmen und entsprechende Empfehlungen abzugeben.
4. Im Bereich der Geheimhaltung muß bei der Auswahl der schutzbedürftigen Informationen und Materialien und bei der Bewertung des Ausmaßes des erforderlichen Schutzes mit Sorgfalt vorgegangen und auf Erfahrungen zurückgegriffen werden. Es ist von entscheidender Bedeutung, daß der Umfang des Schutzes der Sicherheitseinstufung der zu schützenden Informationen und Materialien entspricht. Im Interesse eines reibungslosen Informationsflusses muß dafür gesorgt werden, daß eine zu hohe Einstufung von Verschlußsachen vermieden wird. Das Einstufungssystem ist das Instrument, mit dem diesen Grundsätzen Wirkung verliehen wird. Dasselbe Einstufungssystem sollte bei der Planung und Organisierung von Maßnahmen zur Bekämpfung von Spionage, Sabotage, Terrorismus und anderen Arten der Bedrohung angewandt werden, so daß

die wichtigsten Gebäude, in denen ESA-Verschlußsachen aufbewahrt werden, und die sensibelsten Punkte innerhalb dieser Gebäude auch den größten Schutz erhalten.

Regeln für die Einstufung als Verschlußsache

5. Geheimhaltungsgrade

Verschlußsachen werden wie folgt eingestuft:

„ESA STRENG GEHEIM“ (ESA TS): Dieser Geheimhaltungsgrad findet nur auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der ESA und/oder eines oder mehrerer ihrer Mitgliedstaaten einen äußerst schweren Schaden zufügen könnte.

„ESA GEHEIM“ (ESA S): Dieser Geheimhaltungsgrad findet nur auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der ESA und/oder eines oder mehrerer ihrer Mitgliedstaaten schweren Schaden zufügen könnte.

„ESA VERTRAULICH“ (ESA C): Dieser Geheimhaltungsgrad findet auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der ESA und/oder eines oder mehrerer ihrer Mitgliedstaaten schaden könnte.

„ESA NUR FÜR DEN DIENSTGEBRAUCH“ (ESA R): Dieser Geheimhaltungsgrad findet auf Informationen und Material Anwendung, deren unbefugte Weitergabe für die Interessen der ESA und/oder eines oder mehrerer ihrer Mitgliedstaaten nachteilig sein könnte.

6. Informationen sind nur dann als Verschlußsachen einzustufen, wenn dies nötig ist. Der Geheimhaltungsgrad ist klar und korrekt anzugeben und nur so lange beizubehalten, wie die Informationen geschützt werden müssen.
7. Die Verantwortung für die Festlegung des Geheimhaltungsgrades einer Information liegt allein beim Urheber der Information. ESA-Verschlußsachen dürfen nur mit vorheriger schriftlicher Zustimmung des Urhebers und erforderlichenfalls nach Erörterung mit den übrigen beteiligten Parteien herabgestuft werden; das Gleiche gilt für die Aufhebung des Geheimhaltungsgrades.

GRUNDPRINZIPIEN

8. Die Sicherheitsmaßnahmen sollen
   a) alle Personen, die Zugang zu ESA-Verschlußsachen haben, die Träger von Verschlußsachen und alle Gebäude, in denen sich derartige Verschlußsachen und wichtige Einrichtungen befinden, umfassen;
   b) so ausgelegt sein, daß Personen, die aufgrund ihrer Stellung die Sicherheit von Verschlußsachen und wichtigen Einrichtungen, in denen Verschlußsachen aufbewahrt werden, gefährden könnten, erkannt und vom Zugang ausgeschlossen oder ferngehalten werden;
   c) verhindern, daß unbefugte Personen Zugang zu ESA-Verschlußsachen oder zu Einrichtungen, in denen sie aufbewahrt werden, erhalten;
   d) dafür sorgen, daß ESA-Verschlußsachen nur unter Beachtung des für alle Aspekte der Sicherheit grundlegenden Prinzips „Kenntnis nur wenn nötig“ verbreitet werden;
   e) die Integrität (d.h. Verhinderung von Verfälschungen, unbefugten Änderungen oder unbefugten Löschungen) und die Verfügbarkeit (d.h. keine Verweigerung des Zugangs für Personen, die ihn benötigen und dazu befugt sind) aller ESA-Verschlußsachen und insbesondere der in elektromagnetischer Form gespeicherten, verarbeiteten oder übermittelten Informationen gewährleisten.

ORGANISATION DER SICHERHEIT

9. Der Generaldirektor der ESA und jeder Mitgliedstaat sorgen dafür, daß von allen nationalen Stellen sowie von der Hauptverwaltung, den Niederlassungen und Anlagen der ESA und Vertragspartnern gemeinsame Mindestnormen für die Sicherheit eingehalten werden, so daß bei der Weitergabe von ESA-Verschlußsachen darauf vertraut werden kann, daß diese mit derselben Sorgfalt behandelt werden. Zu diesen Mindestnormen gehören Kriterien für die Sicherheitsüberprüfung des Personals und Verfahren für den Schutz von ESA-Verschlußsachen.
10. Für die ESA ist der Generaldirektor insbesondere damit betraut,
    a) die Sicherheitsvorschriften der ESA anzuwenden;
    b) die Sicherheitsprobleme zu prüfen, mit denen die Hauptverwaltung, die Niederlassungen und die Anlagen der ESA ihn befassen;
    c) Fragen, die Änderungen der Sicherheitsvorschriften der ESA betreffen, in enger Verbindung mit den NSA/DSA oder anderen zuständigen nationalen Behörden der Mitgliedstaaten zu prüfen.

11. Der ESA-Rat setzt einen Sicherheitsausschuß ein. Ihm sollten Delegierte der Mitgliedstaaten angehören, die auch die zuständigen nationalen Sicherheitsbehörden vertreten. Er wird von einem Vorsitzenden und einem Stellvertretenden Vorsitzenden geleitet, die von den Vertretern der Mitgliedstaaten gewählt werden. Der Sicherheitsausschuß berät den ESA-Rat im Rahmen seines Auftrags in allen die Sicherheit betreffenden Fragen.
12. Zur Wahrnehmung der oben genannten Aufgaben steht dem Generaldirektor der ESA das ESA-Sicherheitsbüro zur Verfügung. Der Leiter des ESA-Sicherheitsbüros ist für die Koordinierung, Überwachung und Durchführung von Sicherheitsmaßnahmen einschließlich der Sicherheit von IT-Systemen und -Netzen verantwortlich.
13. In jedem Mitgliedstaat sollte eine für die Sicherheit von ESA-Verschlußsachen zuständige NSA/DSA benannt werden. Diese NSA/DSA sollte insbesondere für folgendes verantwortlich sein:
    a) die Gewährleistung der Sicherheit von ESA-Verschlußsachen, die von einer Stelle oder Einrichtung ihres Landes im In- oder Ausland verwahrt werden;
    b) die Genehmigung der Anlegung eines zentralen Registers für Verschlußsachen, die als „ESA STRENG GEHEIM“ eingestuft sind;
    c) die periodische Überprüfung der Sicherheitsvorkehrungen für den Schutz von ESA-Verschlußsachen;
    d) die Sorge dafür, daß alle in Stellen ihres Landes beschäftigten Personen, die zur Erfüllung ihrer amtlichen Pflichten Zugang zu als „ESA STRENG GEHEIM“, „ESA GEHEIM“ und „ESA VERTRAULICH“ eingestuften ESA-Verschlußsachen haben müssen oder deren Pflichten oder Aufgaben ihnen Zugang zu solchen Verschlußsachen gewähren können, auf angemessene Weise sicherheitsüberprüft werden, bevor sie Zugang zu solchen Verschlußsachen erhalten;
    e) die Aufstellung der Sicherheitspläne, die für erforderlich gehalten werden, um zu verhindern, daß ESA-Verschlußsachen in unbefugte Hände gelangen.
14. Das ESA-Sicherheitsbüro und die zuständige NSA/DSA führen gemeinsam und im beiderseitigen Einvernehmen periodische Inspektionen der Sicherheitsvorkehrungen durch, die in der ESA zum Schutz von ESA-Verschlußsachen getroffen werden.

SICHERHEIT DES PERSONALS

Sicherheitsüberprüfung

15. Der Zugang zu ESA-Verschlußsachen wird nur Personen gestattet, die Kenntnis von ihnen haben müssen, um die ihnen übertragenen Aufgaben oder Aufträge erfüllen zu können. Für die Entscheidung darüber, wer Kenntnis haben muß, sind der Generaldirektor der ESA, der Leiter der ESA-Hauptverwaltung, -Niederlassung und

-Anlage sowie die nationale Stelle, in der die betreffende Person beschäftigt werden soll, entsprechend den Anforderungen der jeweiligen Aufgabe verantwortlich.

16. Alle Personen, die zur Erfüllung ihrer amtlichen Pflichten Zugang zu als *„ESA VERTRAULICH“* oder höher eingestuften ESA-Verschlußsachen haben müssen oder deren Pflichten oder Aufgaben ihnen Zugang zu solchen Verschlußsachen gewähren können, werden einer Sicherheitsüberprüfung unterzogen, bevor sie eine Zugangsermächtigung erhalten. Eine entsprechende Sicherheitsüberprüfung wird auch im Falle von Personen vorgenommen, zu deren Aufgaben der technische Betrieb oder die Wartung von Kommunikations- und Informationssystemen gehört, die Verschlußsachen enthalten.

Bei der Sicherheitsüberprüfung soll insbesondere festgestellt werden, ob die betreffenden Personen

    a) von unzweifelhafter Loyalität sind;
    b) hinsichtlich ihres Charakters und ihrer Diskretionsfähigkeit so beschaffen sind, daß ihre Integrität beim Umgang mit ESA-Verschlußsachen außer Zweifel steht;
    c) eventuell aus dem Ausland oder von anderer Seite her leicht unter Druck gesetzt werden können, z.B. aufgrund ihres früheren Wohnsitzes oder früherer Verbindungen, die ein Sicherheitsrisiko darstellen könnten.

17. Besonders gründlich ist die Sicherheitsüberprüfung bei Personen vorzunehmen, die
    a) Zugang zu Informationen des Geheimhaltungsgrades „ESA STRENG GEHEIM“ erhalten sollen,
    b) Stellen bekleiden, bei denen sie regelmäßig mit einer beträchtlichen Menge an Informationen des Geheimhaltungsgrades „ESA GEHEIM“ zu tun haben;

c) aufgrund ihres Aufgabenbereichs besonderen Zugang zu jeweils entscheidend wichtigen Kommunikations- oder Informationssystemen und somit Gelegenheit haben, sich unbefugt Zugang zu einer größeren Menge von ESA-Verschlußsachen zu verschaffen oder in dem betreffenden Aufgabenbereich durch technische Sabotageakte schweren Schaden zu verursachen.

In den unter den Buchstaben a, b und c genannten Fällen soll soweit als nur möglich auf die Methode der Umfeldermittlung zurückgegriffen werden.

18. Das Sicherheitsüberprüfungsverfahren wird auf Ersuchen des anstellenden Organs durch die NSA/DSA oder eine andere zuständige Behörde des Mitgliedstaats, dessen Staatsangehörigkeit die betreffende Person besitzt, durchgeführt. Hat die betreffende Person ihren Wohnsitz im Hoheitsgebiet eines anderen Mitgliedstaats, können sich die zuständigen nationalen Behörden die Mitwirkung der Behörden des Wohnsitzstaates sichern. Besitzt die Person nicht die Staatsangehörigkeit eines Mitgliedstaats, obliegt die Durchführung des Sicherheitsüberprüfungsverfahrens der NSA/DSA oder der zuständigen nationalen Behörde des Mitgliedstaates, in dem diese Person arbeitet und/oder ihren Wohnsitz hat.
19. Das anstellende Organ benennt in seinem Ersuchen die Art und den Geheimhaltungsgrad der ESA-Verschlußsachen, zu denen die betreffende Person Zugang erhalten soll, damit die NSA/DSA oder die zuständigen nationalen Behörden das Sicherheitsüberprüfungsverfahren durchführen und zu der der betreffenden Person zu erteilenden Ermächtigungsstufe Stellung nehmen können.
20. Für den gesamten Ablauf und die Ergebnisse des Sicherheitsüberprüfungsverfahrens gelten die einschlägigen Vorschriften und Regelungen des betreffenden Mitgliedstaats einschließlich der Vorschriften und Regelungen für etwaige Rechtsbehelfe.
21. Ausnahmsweise kann der Generaldirektor der ESA mit Zustimmung der NSA/DSA oder der zuständigen nationalen Behörde einem Mitglied des ESA-Personals für höchstens sechs Monate eine einstweilige Zugangsermächtigung für Verschlußsachen nur bis zum Geheimhaltungsgrad „ESA GEHEIM“ einschließlich erteilen, bis ihm die Ergebnisse des Sicherheitsüberprüfungsverfahrens vorliegen.

Verzeichnis der Zugangsermächtigungen

22. Nationale Stellen sowie die Hauptverwaltung, Niederlassungen und Anlagen der ESA oder Vertragspartner, die mit ESA-Verschlußsachen zu tun haben oder jeweils entscheidend wichtige Kommunikations- und Informationssysteme verwalten, führen ein Verzeichnis der Zugangsermächtigungen des bei ihnen arbeitenden Personals. Jede Zugangsermächtigung ist erforderlichenfalls zu überprüfen, um sicherzustellen, daß sie der derzeitigen Tätigkeit der betreffenden Person entspricht; sie ist vorrangig zu überprüfen, wenn neue Informationen eingehen, denen zufolge eine weitere Beschäftigung dieser Person mit Verschlußsachen nicht länger mit den Sicherheitsinteressen vereinbar ist. Das Verzeichnis der Zugangsermächtigungen ist vom Sicherheitsbeauftragten der betreffenden nationalen Stelle, ESA-Hauptverwaltung, -Niederlassung und -Einrichtung oder des betreffenden Vertragspartners zu führen.

Sicherheitsanweisungen für das Personal

23. Alle Personen, die Stellen bekleiden, an denen sie Zugang zu Verschlußsachen erhalten könnten, sind bei Aufnahme ihrer Tätigkeit und danach in regelmäßigen Abständen eingehend über die Notwendigkeit von Sicherheitsbestimmungen und über die Verfahren zu ihrer Durchführung zu unterrichten. Alle diese Personen sollten schriftlich bestätigen, daß sie die für ihre Arbeit relevanten Sicherheitsbestimmungen in vollem Umfang verstehen.

Verantwortung der Führungskräfte

24. Führungskräfte haben die Pflicht, sich Kenntnis darüber zu verschaffen, welche ihrer Mitarbeiter mit Verschlußsachen zu tun haben oder über einen Zugang zu jeweils entscheidend wichtigen Kommunikations- oder Informationssystemen verfügen, sowie alle Vorfälle oder offensichtlichen Schwachpunkte von Personen, die sicherheitsrelevant sein können, festzuhalten und darüber zu berichten.

Sicherheitsstatus des Personals

25. Es sind Verfahren vorzusehen, um dafür zu sorgen, daß bei Bekanntwerden nachteiliger Informationen über eine Person festgestellt wird, ob diese Person mit Verschlußsachen zu tun hat oder über einen Zugang zu jeweils entscheidend wichtigen Kommunikations- oder Informationssystemen verfügt, und daß die betreffende Behörde hiervon unterrichtet wird. Ist klar erwiesen, daß

die fragliche Person ein Sicherheitsrisiko darstellt, ist sie von Aufgaben, bei denen sie die Sicherheit gefährden könnte, auszuschließen oder fern zu halten.

„ESA STRENG GEHEIM“-REGISTRATUREN

26. Durch “ESA STRENG GEHEIM”-Registraturen ist sicherzustellen, daß die Registrierung, Handhabung und Verteilung von „ESA STRENG GEHEIM”-Dokumenten gemäß den Sicherheitsvorschriften der ESA erfolgt.
27. Die Zentralregistraturen sind die hauptsächlichen Empfangs- und Versandstellen in den Mitgliedstaaten und in der ESA-Hauptverwaltung, in denen solche Registraturen eingerichtet sind.

VERLETZUNG DER SICHERHEIT UND KENNTNISNAHME VON ESA-VERSCHLUSSSACHEN DURCH UNBEFUGTE

28. Zu einer Verletzung der Sicherheit kommt es, wenn durch eine Handlung oder durch eine Unterlassung, die den Sicherheitsvorschriften der ESA oder eines der Mitgliedstaaten zuwiderläuft, ESA-Verschlußsachen in Gefahr geraten oder Unbefugten zur Kenntnis gelangen.
29. Eine Kenntnisnahme von ESA-Verschlußsachen durch Unbefugte liegt vor, wenn die Verschlußsachen ganz oder teilweise in die Hände unbefugter Personen (d.h. von Personen, die nicht die erforderliche Zugangsermächtigung haben oder deren Kenntnis der Verschlußsachen nicht nötig ist) gelangt ist oder es wahrscheinlich ist, daß eine solche Kenntnisnahme stattgefunden hat.
30. Die Kenntnisnahme von ESA-Verschlußsachen durch Unbefugte kann die Folge von Nachlässigkeit, Fahrlässigkeit oder Indiskretion, aber auch der Tätigkeit von Diensten, die in der ESA oder ihren Mitgliedstaaten Kenntnis von ESA-Verschlußsachen und geheimen Tätigkeiten erlangen wollen, oder von subversiven Organisationen sein.
31. Jede Sicherheitsbehörde hat die Pflicht, unmittelbar nach ihrer Unterrichtung von einer möglichen Sicherheitsverletzung hierüber dem Sicherheitsbüro der ESA Bericht zu erstatten.
32. Gegen jede für die Kenntnisnahme von ESA-Verschlußsachen durch Unbefugte verantwortliche Person können disziplinarische Maßnahmen aufgrund der geltenden Vorschriften und Regelungen ergriffen werden. Diese Maßnahmen lassen etwaige andere rechtliche Verfahren unberührt. Die Mitglieder des ESA-Personals sind von den möglichen rechtlichen Folgen von Verletzungen der Sicherheit und vor allem von der in Artikel 7 des ESA-Sicherheitsübereinkommens vorgesehenen Möglichkeit der Aufhebung ihrer Immunität in Kenntnis zu setzen.

MATERIELLER GEHEIMSCHUTZ

Schutzbedarf

33. Der Umfang der anzuwendenden Maßnahmen des materiellen Geheimschutzes zur Gewährleistung des Schutzes von ESA-Verschlußsachen muß in angemessenem Verhältnis zum Geheimhaltungsgrad, zum Umfang und zur Bedrohung der entsprechenden Informationen und Materialien stehen. Es ist daher darauf zu achten, daß weder eine zu hohe noch eine zu niedrige Einstufung vorgenommen wird und daß die Einstufung regelmäßig überprüft wird. Alle Personen, die ESA-Verschlußsachen verwahren, haben einheitliche Praktiken bei der Einstufung der Informationen anzuwenden und gemeinsame Schutznormen für die Verwahrung, Übermittlung und Vernichtung schutzbedürftiger Informationen und Materialien zu beachten.

Kontrolle

34. Personen, die Bereiche, in denen sich ihnen anvertraute ESA-Verschlußsachen befinden, unbeaufsichtigt lassen, müssen dafür sorgen, daß die Verschlußsachen sicher aufbewahrt und alle Sicherheitsvorkehrungen (Schlösser, Alarm usw.) aktiviert worden sind. Weitere hiervon unabhängige Kontrollen sind nach den Dienststunden durchzuführen.

Gebäudesicherheit

35. Gebäude, in denen sich ESA-Verschlußsachen oder entscheidend wichtige Kommunikations- und Informationssysteme befinden, sind gegen unerlaubten Zutritt zu schützen. Die Art der Schutzmaßnahmen für ESA-Verschlußsachen (z.B. Vergitterung von Fenstern, Schlösser an Türen, Wachen am Eingang, automatische Zugangskontrollsysteme, Sicherheitskontrollen und Rundgänge, Alarmsysteme, Einbruchmeldesysteme und Wachhunde) hängt von folgenden Faktoren ab:
    a) Geheimhaltungsgrad und Umfang der zu schützenden Informationen und Materialien sowie Ort ihrer Unterbringung im Gebäude;
    b) Qualität der Sicherheitsbehältnisse, in denen sich die Informationen und Materialien befinden, und
    c) Beschaffenheit und Lage des Gebäudes.

36. Die Art der Schutzmaßnahmen für Kommunikations- und Informationssysteme hängt in ähnlicher Weise von folgenden Faktoren ab: Einschätzung des Wertes der betreffenden Objekte und der Höhe des im Falle einer Kenntnisnahme durch Unbefugte eventuell entstehenden Schadens; Beschaffenheit und Lage des Gebäudes, in dem das System untergebracht ist; Ort, an dem sich das System innerhalb des Gebäudes befindet.

Notfallpläne

37. Es sind detaillierte Pläne auszuarbeiten, um im Falle eines örtlichen oder nationalen Notstands auf den Schutz von ESA-Verschlußsachen vorbereitet zu sein.

INFORMATIONSSICHERHEIT (INFOSEC)

Grundsätze und Verfahren für die Sicherheit von Systemen

38. Bei allen Kommunikations- und Informationssystemen und -netzen (im folgenden als „SYSTEME“ bezeichnet), in denen ESA-Verschlußsachen verarbeitet werden, sind Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der darin enthaltenen Informationen erforderlich. Alle auf diese Systeme anzuwendenden Sicherheitsmaßnahmen werden von der dazu vorgesehenen Akkreditierungsstelle für IT-Sicherheit (SAA) festgelegt; sie entsprechen dem festgestellten Risiko und stehen mit dem in den Sicherheitsvorschriften der ESA dargelegten Konzept im Einklang.
39. Um ein sicheres Umfeld für den Betrieb eines SYSTEMS zu schaffen, muß eine ausgewogene Kombination von Sicherheitsmaßnahmen ausgewählt und umgesetzt werden. Diese Maßnahmen betreffen physische Objekte, das Personal, nichttechnische Verfahren sowie Betriebsverfahren für Computer und Kommunikationssysteme.
40. Alle SYSTEME, in denen als „ESA VERTRAULICH“ und höher eingestufte Informationen verarbeitet werden, bedürfen der Akkreditierung.
41. Eine Akkreditierungsstelle für IT-Sicherheit (SAA) hat sicherzustellen, daß SYSTEME den Sicherheitsvorschriften der ESA entsprechen.
42. Bei SYSTEMEN, die der ESA gehören, gilt für die SAA folgendes:

– für ein von der Hauptverwaltung, Niederlassungen und Einrichtungen der ESA benutztes SYSTEM:

- Ist das SYSTEM nicht mit einem nationalen Informationssystem verbunden und verwendet oder verarbeitet nicht nationale Verschlußsachen, ist die Akkreditierung ein interner Vorgang;
- andernfalls führt ein Gremium aus Vertretern der ESA und der zuständigen NSA/DSA (der Mitgliedstaaten, die durch die Verbindung oder nationale Einstufung betroffen sind) das Akkreditierungsverfahren durch und erteilt den Akkreditierungsbescheid.

– Für von nationalen Stellen oder Vertragspartnern benutzte SYSTEME wird die Aufgabe der SAA von der NSA/DSA des Mitgliedstaats wahrgenommen, in dem das SYSTEM errichtet ist. In diesem Fall führt die NSA/DSA das Akkreditierungsverfahren durch und erteilt den Akkreditierungsbescheid.

43. Für alle SYSTEME, in denen als „ESA VERTRAULICH“ und höher eingestufte Informationen verarbeitet werden, ist eine Aufstellung der systemspezifischen Sicherheitsanforderungen (SYSTEM-specific Security Requirement Statement, SSRS) erforderlich, die von der SAA zu genehmigen ist.
44. Die Nutzer des SYSTEMS müssen sich erfolgreich einer Sicherheitsüberprüfung unterzogen haben, die dem Geheimhaltungsgrad der in ihrem jeweiligen SYSTEM verarbeiteten Informationen entspricht, und sie müssen einen entsprechenden berechtigten Informationsbedarf haben. Der Zugang zu bestimmten (z.B. kryptografischen) Geräten oder Informationen, die für die SYSTEME sicherheitsrelevant sind, erfordert eine besondere Ermächtigung, die von der zuständigen NSA/DSA erteilt wird.

MASSNAHMEN GEGEN SABOTAGE UND ANDERE FORMEN VORSÄTZLICHER BESCHÄDIGUNG

45. Vorsichtsmaßnahmen im Bereich des Objektschutzes zum Schutz wichtiger Einrichtungen, in denen Verschlußsachen untergebracht sind, sind die besten Sicherheitsgarantien gegen Sabotage und vorsätzliche Beschädigungen; eine Sicherheitsüberprüfung des Personals allein ist kein wirklicher Ersatz.

INDUSTRIELLE SICHERHEIT

46. Alle Einrichtungen, die an industriellen Tätigkeiten mit Zugang zu als „ESA VERTRAULICH“ und höher eingestuften Informationen teilnehmen, müssen einen Sicherheitsbescheid für Einrichtungen (Facility Security Clearance, FSC) besitzen.
47. Für alle als „ESA VERTRAULICH“ und höher eingestuften Verträge teilt der Hauptauftragnehmer der NSA/DSA der Nation, in der die Einrichtung, an die der Vertrag vergeben wurde, angesiedelt oder eingetragen ist, mit, daß dieser Einrichtung zusammen mit dem Vertrag eine Geheimschutzklausel (Security Aspect Letter, SAL) übermittelt worden ist.
48. Der Hauptauftragnehmer wird vertraglich unter Androhung der Kündigung seines Vertrags verpflichtet, alle von der ESA und/oder den NSA/DSA vorgeschriebenen Maßnahmen zum Schutz der ESA-Verschlußsachen, die von dem Auftragnehmer hervorgebracht oder ihm anvertraut werden oder in von ihm hergestellte Gegenstände eingehen, zu ergreifen.
49. Der Hauptvertrag enthält als Anlage eine Sicherheitsanweisung für Vorhaben (PSI). Ein „Einstufungsleitfaden für VS-Vorhaben“ ist Bestandteil der PSI. Alle anderen als Verschlußsache eingestuften ESA-Verträge enthalten mindestens eine „Geheimschutzklausel“ (SAL). Im letzteren Fall kann der Einstufungsleitfaden für VS-Vorhaben als „VS-Einstufungsliste“ bezeichnet werden. Die PSI und/oder SAL bilden das für die Sicherheit des Vertrags maßgebliche einheitliche Dokument.
50. Der Hauptauftragnehmer kann Unterverträge mit anderen Auftragnehmern, d.h. Unterauftragnehmern, aushandeln. Diese Unterauftragnehmer können ihrerseits Unteraufträge mit anderen Unterauftragnehmern aushandeln. Der Hauptauftragnehmer ist für alle Unterauftragstätigkeiten verantwortlich.
51. Für als „ESA VERTRAULICH“ und höher eingestufte Verträge müssen alle Auftragnehmer stets Inhaber eines FSC sein und dafür sorgen, daß ihre an den Verhandlungen beteiligten Vertreter Inhaber eines entsprechenden PSC (Sicherheitsbescheid für Personen) sind und nur Zugang zu den für die Aushandlung des Vertrags erforderlichen ESA-Verschlußsachen erhalten. Für als „ESA NUR FÜR DEN DIENSTGEBRAUCH“ eingestufte Verträge ist ein FSC nicht notwendig, sofern nicht nationale Sicherheitsvorschriften und -regelungen ihn ausdrücklich vorschreiben.
52. Anträge für die Sicherheitsüberprüfung von Personal der Auftragnehmereinrichtungen sind an die NSA/DSA, die für die Einrichtung verantwortlich ist, zu richten. In einem Antrag auf Überprüfung oder Erteilung eines PSC sind anzugeben:
    a) die Bezeichnung und Sicherheitseinstufung des Vertrags oder Untervertrags und
    b) der Geheimhaltungsgrad der ESA-Verschlußsachen, zu denen die betreffende Person Zugang haben wird.
53. Wünscht eine Einrichtung einen Staatsangehörigen eines ESA-Nichtmitgliedstaats in einer Stellung zu beschäftigen, die Zugang zu ESA-Verschlußsachen erfordert, ist die NSA/DSA des Mitgliedstaats, in dem sich die anstellende Einrichtung befindet, für die Durchführung des hier beschriebenen Sicherheitsüberprüfungsverfahrens und für die Entscheidung darüber verantwortlich, ob der betreffenden Person im Einklang mit den ESA-Sicherheitsvorschriften, insbesondere Teil I Abschnitt 8, Zugang gewährt werden kann.

AUSTAUSCH VON VERSCHLUSSSACHEN ZWISCHEN DER ESA UND DRITTSTAATEN ODER INTERNATIONALEN ORGANISATIONEN

54. Über den Austausch von ESA-Verschlußsachen mit Drittstaaten, internationalen Organisationen oder anderen Dritten entscheidet der ESA-Rat.
55. Hat der ESA-Rat entschieden, daß eine ständige oder langfristige oder fallweise Notwendigkeit für den Austausch von Verschlußsachen zwischen der ESA und Drittstaaten oder anderen internationalen Organisationen besteht, handelt der Generaldirektor der ESA mit ihnen Vereinbarungen über Sicherheitsverfahren für den Austausch von Verschlußsachen oder Abmachungen aus, die den Zweck der Zusammenarbeit und die gegenseitigen Vorschriften für den Schutz der ausgetauschten Informationen festlegen.
56. Der Entwurf der Vereinbarungen über Sicherheitsverfahren oder der Abmachungen ist vom Sicherheitsausschuß zu billigen, bevor er dem ESA-Rat zur Beschlußfassung unterbreitet wird.
57. Die Durchführung der Verfahren für die Weitergabe von ESA-Verschlußsachen, die von der ESA stammen, an einen Drittstaat oder eine internationale Organisation obliegt dem Generaldirektor. Stammen die Verschlußsachen, um deren Weitergabe ersucht wird, nicht von der ESA, hat der Generaldirektor zunächst die schriftliche Zustimmung des Urhebers der Verschlußsache einzuholen. Kann dieser Urheber nicht ermittelt werden, trifft das zuständige ESA-Gremium an seiner Stelle die Entscheidung.

ANLAGE

58. Eine Vergleichstabelle der Sicherheitseinstufungen der ESA und der Mitgliedstaaten ist in der Anlage enthalten.

GLOSSAR DER VERWENDETEN BEGRIFFE

Akkreditierung bezeichnet den Vorgang, der bestätigt, daß ein SYSTEM unter den in der Aufstellung der Systemspezifischen Sicherheitsanforderungen (SSRS) oder in einem anderen einschlägigen Dokument festgelegten Sicherheitsbedingungen betrieben wird und kein unannehmbares Risiko darstellt.

Anstellendes Organ bezeichnet das Organ, das befugt ist, eine Person anzustellen und um ihre Sicherheitsüberprüfung zu ersuchen.

Verfügbarkeit bedeutet, daß die Informationen und Materialien einer befugten Person oder Einrichtung auf Verlangen zugänglich sind und von ihr genutzt werden können.

Zuständige Behörde bezeichnet eine von der NSA eines Mitgliedstaates bestimmte Behörde, die zur Durchführung von Sicherheitsüberprüfungen befugt ist, um seinen Staatsangehörigen Zugang zu ESA-Verschlußsachen zu gewähren.

Auftragnehmer bezeichnet eine juristische Person oder Stelle, die sich bereit erklärt, als Haupt-, Einzel- oder Unterauftragnehmer Güter zu liefern oder Dienste zu erbringen.

Benannte Sicherheitsbehörde bezeichnet eine Behörde, die gegenüber der Nationalen Sicherheitsbehörde (NSA) eines Mitgliedstaates unter anderem für die Unterrichtung der Industrie über die nationale Politik in allen Fragen der industriellen Sicherheitspolitik der ESA und für Weisungen und Unterstützung bei ihrer Umsetzung verantwortlich ist. In manchen Ländern kann die Aufgabe einer DSA von der NSA wahrgenommen werden.

Einrichtung bezeichnet eine juristische Person oder Stelle.

ESA-Verschlußsachen bezeichnet alle Informationen, Dokumente oder Materialien gleich welcher Form, deren unbefugte Weitergabe den Interessen einer oder mehrerer Vertragsparteien des ESA-Sicherheitsübereinkommens schaden könnte und die durch eine Sicherheitseinstufung als solche gekennzeichnet wurden, unabhängig davon, ob diese Informationen von der ESA stammen oder der ESA von einem Mitgliedstaat zugeleitet werden oder von einem Mitgliedstaat einem anderen Mitgliedstaat zur Unterstützung eines Programms, Projekts oder Vertrags der ESA zugeleitet werden.

ESA-Sicherheitsüberprüfung bezeichnet die Feststellung, daß einer Person Zugang zu ESA-Verschlußsachen gewährt werden darf.

ESA-Sicherheitsübereinkommen bezeichnet das Übereinkommen zwischen den Vertragsstaaten des Übereinkommens zur Gründung einer Europäischen Weltraumorganisation und der Europäischen Weltraumorganisation für den Schutz und Austausch von der Geheimhaltung unterliegenden Informationen, das vom ESA-Rat am 13. Juni 2002 genehmigt wurde.

Mitglied des ESA-Personals bezeichnet eine nach Artikel XII Absatz 3 des ESA-Übereinkommens angestellte Person, deren Beschäftigungsbedingungen der Personalordnung der ESA und den zugehörigen Durchführungsbestimmungen und -richtlinien unterliegen.

Sicherheitsbescheid für Einrichtungen (FSC) bezeichnet die verwaltungsrechtliche Feststellung durch eine NSA/DSA, daß eine Einrichtung unter dem Gesichtspunkt der Sicherheit ausreichenden Schutz für ESA-Verschlußsachen eines festgelegten Geheimhaltungsgrads oder darunter bietet und ihr Personal, das Zugang zu ESA-Verschlußsachen haben muß, ordnungsgemäß sicherheitsüberprüft und von den bei ESA-Verträgen, die als Verschlußsache eingestuft sind, zu beachtenden Sicherheitsanforderungen der ESA unterrichtet wurde.

INFOSEC bezeichnet die Anwendung von Sicherheitsmaßnahmen zum Schutz von Informationen, die in Kommunikations-, Informations- und anderen elektronischen Systemen verarbeitet, gespeichert oder übermittelt werden, vor dem absichtlichen oder unabsichtlichen Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit sowie zur Vermeidung des Verlusts der Integrität oder Verfügbarkeit der Systeme selbst.

Anmerkungen:

1. INFOSEC-Maßnahmen erstrecken sich auf die Sicherheit von Computern, die Sicherheit der Übertragung, die Sicherheit vor Abstrahlung und die kryptografische Sicherheit.
2. Diese Maßnahmen schließen auch die Aufdeckung, Dokumentation und Bekämpfung von Bedrohungen für Informationen und Systeme ein.

Mitgliedstaat bezeichnet einen Staat, der Vertragsstaat des Übereinkommens zur Gründung einer Europäischen Weltraumorganisation im Sinne seiner Artikel XX und XXII ist.

Nationale Stelle bezeichnet eine Abteilung, ein Büro, einen Dienst oder eine Einrichtung einer Verwaltungs- oder Regierungsstelle eines Mitgliedstaats.

Nationale Sicherheitsbehörde bezeichnet eine Behörde eines Mitgliedstaats, die für die Gewährleistung der Sicherheit von ESA-Verschlußsachen bei nationalen Stellen im In- und Ausland verantwortlich ist.

Das **Prinzip „Kenntnis nur wenn nötig“** bezeichnet den Grundsatz, nach dem die positive Feststellung getroffen wird, daß ein vorgesehener Empfänger den Zugang zu, die Kenntnis oder den Besitz von Informationen benötigt, um die ihm übertragenen Aufgaben oder Aufträge erfüllen zu können.

Einstufungsleitfaden für VS-Vorhaben bezeichnet den Teil der Sicherheitsanweisung für Vorhaben (PSI), der die als Verschlußsachen eingestuften Teile eines Vorhabens unter Angabe der Geheimhaltungsgrade ausweist. Der Einstufungsleitfaden für VS-Vorhaben kann während der Laufzeit des Vorhabens erweitert werden, und Teile der Informationen können neu eingestuft oder herabgestuft werden.

Sicherheitsanweisung für Vorhaben bezeichnet eine Aufstellung der Sicherheitsvorschriften/-verfahren, die auf ein bestimmtes Vorhaben anzuwenden sind, um die Sicherheitsverfahren zu vereinheitlichen. Die PSI bildet auch eine Anlage zum Hauptvertrag und kann während der Laufzeit des Vorhabens geändert werden. Für im Rahmen des Vorhabens vergebene Unterverträge stellt die PSI die Grundlage für die Geheimschutzklausel dar.

Geheimschutzklausel bezeichnet ein von der zuständigen Stelle erstelltes Dokument, das Bestandteil aller als Verschlußsache eingestuften Verträge und Unterverträge ist und die Anforderungen an den Sicherheitsschutz festlegt oder die schutzbedürftigen Teile der Verträge oder Unterverträge bestimmt.

Annex 5

VERGLEICH MIT DEN NATIONALEN SICHERHEITSEINSTUFUNGEN				
ESA-Einstufung	ESA STRENG GEHEIM	ESA GEHEIM	ESA VERTRAULICH	ESA NUR FÜR DEN DIENSTGEBRAUCH
Belgien	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Dänemark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Deutschland	Streng Geheim	Geheim	VS[3] - Vertraulich	VS – Nur für den Dienstgebrauch
Spanien	Secreto	Reservado	Confidencial	Difusion limitada
Frankreich	Très Secret Défense[4]	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irland	Top Secret	Secret	Confidential	Restricted
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Niederlande	STG Zeer Geheim	STG Geheim	STG Confidentieel	
Norwegen	Strengt Hemmelig	Hemmelig	Konfidensielt	Begrenset
Österreich	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finnland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Schweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Schweiz	Geheim Secret	Geheim Secret	Vertraulich Confidentiel	Vertraulich Confidentiel
Vereinigtes Königreich	Top Secret	Secret	Confidential	Restricted

[1]Deutschland: VS = Verschlusssache
[2]Frankreich: Die Einstufung “Très Secret Défense”, die für Regierungsprioritäten gilt, darf nur mit Zustimmung des Premierministers geändert werden.

Annex 5

Anlage 2 Teil II der Erläuterungen

SICHERHEITSVORSCHRIFTEN DER ESA – TEIL II

ABSCHNITT I

DIE ORGANISATION DER SICHERHEIT IN DER EUROPÄISCHEN WELTRAUMORGANISATION

Der Generaldirektor

1. Der Generaldirektor nimmt in Absprache mit dem unter den Nummern 3 und 4 genannten Sicherheitsausschuss der ESA folgende Aufgaben wahr:
   a) Er wendet die Sicherheitsvorschriften der ESA an;
   b) er befasst sich mit Sicherheitsproblemen, die die Hauptverwaltung, Niederlassungen und Anlagen der ESA ihm vorlegen;
   c) er prüft in enger Abstimmung mit den Nationalen Sicherheitsbehörden/Benannten Sicherheitsbehörden (NSA/DSA) oder sonstigen zuständigen Behörden der Mitgliedstaaten Fragen, die eine Änderung der Sicherheits-vorschriften der ESA erforderlich machen.
2. Der Generaldirektor ist insbesondere für folgendes zuständig:
   a) Er koordiniert alle die Tätigkeiten der ESA betreffenden Sicherheitsfragen;
   b) er trifft die erforderlichen Maßnahmen zur Anlegung eines Zentralregisters der als „ESA STRENG GEHEIM“ eingestuften Verschlusssachen in der Hauptverwaltung, den Niederlassungen und den Anlagen der ESA;
   c) er richtet an die zuständigen Behörden der Mitgliedstaaten Anträge auf Sicherheitsüberprüfung von Bediensteten und Sachverständigen der ESA durch die jeweilige NSA im Einklang mit Abschnitt VI;
   d) er ermittelt oder ordnet Ermittlungen an, wenn ESA-Verschlusssachen Unbefugten zur Kenntnis gelangt sind und die Ursache hierfür dem ersten Anschein nach in der Hauptverwaltung, den Niederlassungen oder den Anlagen der ESA zu suchen ist;
   e) er ersucht die entsprechenden Sicherheitsbehörden um die Einleitung von Ermittlungen, wenn eine Kenntnisnahme von ESA-Verschlusssachen durch Unbefugte außerhalb der Hauptverwaltung, den Niederlassungen oder den Anlagen der ESA erfolgt zu sein scheint, und koordiniert die Ermittlungen in den Fällen, in denen mehr als eine Sicherheitsbehörde beteiligt ist;
   f) er überprüft gemeinsam und im Einvernehmen mit den betreffenden NSA periodisch die Sicherheitsvorkehrungen zum Schutz von ESA-Verschlusssachen in den Mitgliedstaaten;
   g) er unterhält enge Verbindungen zu allen betroffenen Sicherheitsbehörden, um für eine Gesamtkoordinierung der Sicherheitsmaßnahmen zu sorgen;
   h) er behält ständig die Sicherheitsvorschriften und -verfahren der ESA im Auge und arbeitet gegebenenfalls entsprechende Empfehlungen aus. In diesem Zusammenhang legt er dem Rat der ESA den vom ESA-Sicherheitsbüro erstellten jährlichen Inspektionsplan vor.

Der Sicherheitsausschuss

3. Mit der ESA-Ratsentschließung ESA/C/R/CLIX/Res.1 (Final) vom 13. Juni 2002 wurde ein Sicherheitsausschuss eingesetzt. Diesem Ausschuss sollen Delegierte der Mitgliedstaaten angehören, die auch die zuständigen nationalen Sicherheitsbehörden vertreten und nach Bedarf Berater hinzuziehen können. Der Sicherheitsausschuss wird von einem Vorsitzenden und einem Stellvertretenden Vorsitzenden geleitet, die aus den Vertretern der Mitgliedstaaten gewählt werden.
4. Entsprechend seinem Auftrag berät der Sicherheitsausschuss den Rat und den Generaldirektor der ESA in allen die Sicherheit betreffenden Fragen und bereitet Beschlüsse hierüber vor, die er dem Rat zur Genehmigung empfiehlt.

Das ESA-Sicherheitsbüro

5. Dem Generaldirektor steht bei der Wahrnehmung seiner unter den Nummern 1 und 2 genannten Aufgaben das ESA-Sicherheitsbüro für die Koordinierung, Überwachung und Durchführung von Sicherheitsmaßnahmen zur Verfügung.
6. Der Leiter des ESA-Sicherheitsbüros berät den Generaldirektor in Sicherheitsfragen und fungiert als Sekretär des Sicherheitsausschusses. In dieser Hinsicht leitet er die Aktualisierung der Si-

cherheitsvorschriften und koordiniert die Sicherheitsmaßnahmen mit den zuständigen Behörden der Mitgliedstaaten und gegebenenfalls mit internationalen Organisationen, die Sicherheitsabkommen mit der ESA geschlossen haben. Er hat hierbei die Rolle einer Verbindungsperson.

7. Der Leiter des ESA-Sicherheitsbüros ist für die Zulassung von IT-Systemen und -Netzen in der ESA verantwortlich. Der Leiter des ESA-Sicherheitsbüros und die zuständigen NSA entscheiden gegebenenfalls gemeinsam über die Zulassung von IT-Systemen und -Netzen, die die Hauptverwaltung, Niederlassungen und Anlagen der ESA und andere Empfänger von ESA-Verschlusssachen umfassen.

Die Hauptverwaltung, Niederlassungen und Anlagen der ESA

8. Die Abteilung Standortverwaltung ist unter der Leitung des ESA-Sicherheitsbüros für die Durchführung von materiellen Sicherheitsmaßnahmen in der Hauptverwaltung, den Niederlassungen und den Anlagen der ESA zuständig. Der Leiter der Abteilung Standortverwaltung bestimmt einen seiner Mitarbeiter als den ihm rechenschaftspflichtigen Verantwortlichen für diesen Bereich. Der betreffende Mitarbeiter wird zum Standortsicherheitsbeauftragten ernannt.

Die Mitgliedstaaten

9. Jeder Mitgliedstaat sollte eine für die Sicherheit von ESA-Verschlusssachen zuständige NSA benennen.
10. Innerhalb der Verwaltungsstruktur der einzelnen Mitgliedstaaten sollte die jeweilige NSA für folgendes zuständig sein:
    a) die Gewährleistung der Sicherheit von ESA-Verschlusssachen, die von einer Stelle oder Einrichtung ihres Landes im In- oder Ausland verwahrt werden;
    b) die Genehmigung der Anlegung von „ESA STRENG GEHEIM“-Registern (diese Genehmigungsbefugnis kann auch auf den in einer Zentralregistratur für als „ESA STRENG GEHEIM“ eingestufte Verschlusssachen zuständigen Kontrollbeauftragten übertragen werden);
    c) die periodische Überprüfung der Sicherheitsvorkehrungen für den Schutz von ESA-Verschlusssachen;
    d) die Sorge dafür, dass alle Personen in einer Stelle ihres Landes, die zur Erfüllung ihrer amtlichen Pflichten Zugang zu als „ESA STRENG GEHEIM“, „ESA GEHEIM“ und „ESA VERTRAULICH“ eingestuften ESA-Verschlusssachen haben müssen oder deren Pflichten oder Aufgaben ihnen Zugang zu solchen Verschlusssachen gewähren können, auf angemessene Weise sicherheitsüberprüft werden, bevor sie Zugang zu solchen Verschlusssachen erhalten;
    e) die Aufstellung der Sicherheitspläne, die für erforderlich gehalten werden, um zu verhindern, dass ESA-Verschlusssachen in unbefugte Hände gelangen.

Gegenseitige Sicherheitsinspektionen

11. Das ESA-Sicherheitsbüro und die jeweilige NSA führen gemeinsam und im beiderseitigen Einvernehmen periodische Inspektionen der Sicherheitsvorkehrungen durch, die zum Schutz von ESA-Verschlusssachen in der ESA getroffen werden.

ABSCHNITT II

GEHEIMHALTUNGSGRADE UND KENNZEICHNUNGEN

GEHEIMHALTUNGSGRADE

Verschlusssachen werden wie folgt eingestuft:

1. **„ESA STRENG GEHEIM“ (ESA TS):** Dieser Geheimhaltungsgrad findet nur auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der ESA und/oder eines oder mehrerer ihrer Mitgliedstaaten einen äußerst schweren Schaden zufügen könnte.
2. **„ESA GEHEIM“ (ESA S):** Dieser Geheimhaltungsgrad findet nur auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der ESA und/oder eines oder mehrerer ihrer Mitgliedstaaten schweren Schaden zufügen könnte.
3. **„ESA VERTRAULICH“ (ESA C):** Dieser Geheimhaltungsgrad findet auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der ESA und/oder eines oder mehrerer ihrer Mitgliedstaaten schaden könnte.

4. **„ESA NUR FÜR DEN DIENSTGEBRAUCH“ (ESA R):** Dieser Geheimhaltungsgrad findet auf Informationen und Material Anwendung, deren unbefugte Weitergabe für die Interessen der ESA und/oder eines oder mehrerer ihrer Mitgliedstaaten nachteilig sein könnte.

KENNZEICHNUNGEN

5. Als Warnhinweis dienende Kennzeichnungen können benutzt werden, um den von einem Dokument abgedeckten Bereich oder eine besondere Verteilung gemäß dem Grundsatz „Kenntnis nur wenn nötig“ anzugeben.
6. Bestimmte Dokumente, insbesondere Dokumente mit Bezug zu Informationstechnologie (IT)-Systemen, können mit einer zusätzlichen Kennzeichnung versehen werden, die in den entsprechenden Regelungen und in Abschnitt XI dieser Vorschriften festgelegte weitere Sicherheitsmaßnahmen zur Folge hat.

ANBRINGUNG EINES HINWEISES AUF DEN GEHEIMHALTUNGSGRAD UND SONSTIGE KENNZEICHNUNGEN

7. Ein Hinweis auf den Geheimhaltungsgrad und sonstige Kennzeichnungen werden wie folgt angebracht:
   a) bei Dokumenten, die als „ESA NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft werden, mit mechanischen oder elektronischen Mitteln;
   b) bei Dokumenten, die als „ESA VERTRAULICH“ eingestuft werden, mit mechanischen Mitteln und von Hand oder durch Druck auf vorgestempeltem, registriertem Papier;
   c) auf Dokumenten, die als „ESA GEHEIM“ oder „ESA STRENG GEHEIM“ eingestuft werden, mit mechanischen Mitteln und von Hand.

ABSCHNITT III

REGELN FÜR DIE EINSTUFUNG ALS VERSCHLUSSSACHE

1. Informationen sind nur dann als Verschlusssachen einzustufen, wenn dies nötig ist. Der Geheimhaltungsgrad ist klar und korrekt anzugeben und nur so lange beizubehalten, wie die Informationen geschützt werden müssen.
2. Die Verantwortung für die Festlegung des Geheimhaltungsgrades einer Information und für jede anschließende Herabstufung oder Aufhebung des Geheimhaltungsgrades liegt allein beim Urheber der Information. Ist die ESA der Urheber, so werden Einstufungen, Herabstufungen oder Aufhebungen des Geheimhaltungsgrades von Verschlusssachen von den Bediensteten der ESA nur auf Anweisung ihres Direktors oder Abteilungsleiters oder mit dessen Zustimmung vorgenommen.
3. Die Zahl der Personen, die dazu ermächtigt sind, Dokumente des Geheimhaltungsgrades „ESA STRENG GEHEIM“ in Umlauf zu bringen, ist möglichst klein zu halten, und ihre Namen sind in einer Liste zu verzeichnen, die vom Generaldirektor und von jedem Mitgliedstaat geführt wird.

ANWENDUNG DER GEHEIMHALTUNGSGRADE

4. Bei der Festlegung des Geheimhaltungsgrades eines Dokuments wird das Ausmaß der Schutzbedürftigkeit seines Inhalts entsprechend der Definition in Abschnitt II Nummern 1 bis 4 zu Grunde gelegt. Es ist wichtig, dass die Einstufung korrekt vorgenommen wird und nur bei wirklichem Bedarf erfolgt. Dies gilt insbesondere für eine Einstufung als „ESA STRENG GEHEIM“.
5. Der Urheber eines Dokuments, das als Verschlusssache eingestuft werden soll, sollte sich der vorstehend genannten Regelungen bewusst sein und eine zu hohe oder zu niedrige Einstufung vermeiden. Eine hohe Einstufung scheint zwar auf den ersten Blick mehr Schutz für ein Dokument zu garantieren, doch kann die routinemäßige Vornahme einer zu hohen Einstufung dazu führen, dass das Vertrauen in die Gültigkeit des Einstufungssystems verlorengeht. Andererseits sollten Dokumente nicht in der Absicht zu niedrig eingestuft werden, die mit ihrem Schutz verbundenen Zwänge zu vermeiden.
6. Einzelne Seiten, Abschnitte, Teile, Anhänge oder sonstige Anlagen eines Dokuments können eine unterschiedliche Einstufung erforderlich machen und sind entsprechend zu kennzeichnen. Als Geheimhaltungsgrad des Gesamtdokuments gilt mindestens der Geheimhaltungsgrad seines am höchsten eingestuften Teils.
7. Ein Begleitschreiben oder ein Übermittlungsvermerk ist so hoch einzustufen wie die am höchsten eingestufte Anlage. Der Urheber sollte klar angeben, welcher Geheimhaltungsgrad für das Begleitschreiben bzw. den Übermittlungsvermerk gilt, wenn ihm seine Anlagen nicht beigefügt sind.

HERABSTUFUNG UND AUFHEBUNG DES GEHEIMHALTUNGSGRADES

8. ESA-Verschlusssachen dürfen nur mit vorheriger Zustimmung des Urhebers und erforderlichenfalls nach Erörterung mit den übrigen Beteiligten herabgestuft werden; das gleiche gilt für die Aufhebung des Geheimhaltungsgrades. Die Herabstufung oder Aufhebung des Geheimhaltungsgrades ist schriftlich zu bestätigen. Dem Urheber obliegt es, die Empfänger des Dokuments über die Änderung der Einstufung zu informieren, wobei letztere wiederum die weiteren Empfänger, denen sie das Original oder eine Kopie des Dokuments zugeleitet haben, davon zu unterrichten haben.
9. Soweit möglich gibt die Stelle, von der das Dokument stammt, auf dem als Verschlusssache eingestuften Dokument den Zeitpunkt oder eine Frist an, ab dem/nach deren Ablauf die in dem Dokument enthaltenen Informationen herabgestuft werden können oder deren Geheimhaltungsgrad aufgehoben werden kann. Anderenfalls überprüft sie die Dokumente spätestens alle fünf Jahre, um sich zu vergewissern, dass die ursprüngliche Einstufung nach wie vor erforderlich ist.

ABSCHNITT IV
MATERIELLER GEHEIMSCHUTZ

ALLGEMEINES

1. Hauptziel der Maßnahmen des materiellen Geheimschutzes ist es, zu verhindern, dass Unbefugte Zugang zu ESA-Verschlusssachen erhalten.
2. Die Abteilung Standortverwaltung trifft in enger Abstimmung mit dem Leiter des ESA-Sicherheitsbüros ergänzende Maßnahmen, wenn für geplante Tätigkeiten der ESA (z.B. mit Erprobungen und Starts verbundene Tätigkeiten) eine Verschärfung der in diesem Abschnitt beschriebenen Bestimmungen erforderlich ist.

SICHERHEITSANFORDERUNGEN

3. Alle Gebäude, Bereiche, Büros, Räume, Kommunikations- und Informationssysteme usw., in denen als ESA-Verschlusssache eingestufte Informationen und/oder Material aufbewahrt werden und/oder in denen damit gearbeitet wird, sind durch geeignete Maßnahmen des materiellen Geheimschutzes zu sichern.
4. Bei der Festlegung des erforderlichen materiellen Geheimschutzniveaus ist allen relevanten Faktoren Rechnung zu tragen, wie beispielsweise
   a) der Einstufung der Informationen und/oder des Materials;
   b) der Menge und der Form (z.B. Papier, EDV-Datenträger) der verwahrten Informationen;
   c) der örtlichen Einschätzung der Bedrohung, die gegen die ESA, die Mitgliedstaaten und/oder andere Institutionen oder Dritte gerichtet ist, die ESA-Verschlusssachen verwahren, insbesondere durch Sabotage, Terrorismus, Spionage und andere subversive und/oder kriminelle Handlungen. Diese Einschätzung der Bedrohung wird vom ESA-Sicherheitsbüro mit Unterstützung der Abteilung Standortverwaltung und in enger Abstimmung mit der zuständigen NSA des Landes vorgenommen, in dem die Hauptverwaltung, Niederlassung oder Anlage der ESA angesiedelt ist.
5. Die Maßnahmen des materiellen Geheimschutzes zielen darauf ab,
   a) das heimliche oder gewaltsame Eindringen unbefugter Personen von außen zu verhindern;
   b) von Tätigkeiten illoyaler Bediensteter oder Sachverständiger der ESA (Spionage von innen) abzuschrecken beziehungsweise diese zu verhindern und aufzudecken;
   c) zu verhindern, dass Bedienstete oder Sachverständige der ESA und von nationalen Stellen und/oder Dritten beschäftigte Personen, die die betreffenden Kenntnisse nicht benötigen, Zugang zu ESA-Verschlusssachen erhalten.

MASSNAHMEN DES MATERIELLEN GEHEIMSCHUTZES

Sicherheitsbereiche

6. Die Bereiche, in denen mit als „ESA VERTRAULICH“ oder höher eingestuften Verschlusssachen gearbeitet wird oder in denen diese aufbewahrt werden, sind so zu gestalten und auszustatten, dass sie einer der nachstehenden Kategorien entsprechen:
   a) Sicherheitsbereich der Kategorie I: Bereich, in dem mit als „ESA VERTRAULICH“ oder höher eingestuften Verschlusssachen gearbeitet wird oder diese aufbewahrt werden, wobei das Betreten des Bereichs für alle praktischen Zwecke den Zugang zu den Verschlusssachen ermöglicht. Ein derartiger Bereich erfordert

i) einen klar abgegrenzten und geschützten Raum mit vollständiger Ein- und Ausgangskontrolle;

ii) ein Zutrittskontrollsystem, mit dem dafür gesorgt wird, dass nur die gehörig überprüften und eigens ermächtigten Personen den Bereich betreten können;

iii) eine genaue Festlegung der Einstufung der Verschlusssachen, die in der Regel in dem Bereich verwahrt werden, d.h. der Informationen, die durch das Betreten des Bereichs zugänglich werden.

Bei Personen, die nicht in solchen Bereichen arbeiten, ist eine Begleitung oder eine gleichwertige Kontrolle sicherzustellen, damit der Zugang Unbefugter zu ESA-Verschlusssachen sowie ein unkontrolliertes Betreten von Bereichen, die technischen Sicherheitskontrollen unterliegen, verhindert werden.

b) Sicherheitsbereich der Kategorie II: Bereich, in dem mit als „ESA VERTRAULICH“ oder höher eingestuften Verschlusssachen gearbeitet wird oder diese aufbewahrt werden, wobei durch interne Kontrollen ein Schutz vor dem Zugang Unbefugter ermöglicht wird, beispielsweise Gebäude mit Büros, in denen regelmäßig mit solchen Verschlusssachen gearbeitet wird und in denen diese aufbewahrt werden. Ein derartiger Bereich erfordert

i) einen klar abgegrenzten und geschützten Raum mit vollständiger Ein- und Ausgangskontrolle;

ii) ein Zutrittskontrollsystem, mit dem dafür gesorgt wird, dass nur die gehörig überprüften und eigens ermächtigten Personen den Bereich unbegleitet betreten können. Bei allen anderen Personen ist eine Begleitung oder eine gleichwertige Kontrolle sicherzustellen, damit der Zugang Unbefugter zu ESA-Verschlusssachen sowie ein unkontrolliertes Betreten von Bereichen, die technischen Sicherheitskontrollen unterliegen, verhindert werden.

Die Bereiche, die nicht rund um die Uhr von diensttuendem Personal besetzt sind, sind unmittelbar nach den üblichen Arbeitszeiten zu inspizieren, um sicherzustellen, dass die ESA-Verschlusssachen ordnungsgemäß gesichert sind.

Verwaltungsbereich

7. Um die Sicherheitsbereiche der Kategorien I und II herum oder im Zugangsbereich zu ihnen kann ein Verwaltungsbereich mit geringerem Sicherheitsgrad vorgesehen werden. Ein derartiger Bereich erfordert einen deutlich abgegrenzten Raum, der die Kontrolle des Personals und der Fahrzeuge ermöglicht. In den Verwaltungsbereichen darf nur mit als „ESA NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Verschlusssachen gearbeitet werden, und es dürfen auch nur diese Verschlusssachen dort aufbewahrt werden.

Ein- und Ausgangskontrollen

8. Das Betreten der Sicherheitsbereiche der Kategorien I und II wird mittels eines Berechtigungsausweises oder eines Systems zur persönlichen Identifizierung kontrolliert. Eine Regelung mit Berechtigungsausweisen kann durch eine automatisierte Erkennung unterstützt werden, die als Ergänzung zum Einsatz des Personals des Sicherheitsdienstes zu verstehen ist, diesen aber nicht vollständig ersetzen kann.

9. Ferner wird ein Kontrollsystem für Besucher eingerichtet, damit der Zugang Unbefugter zu ESA-Verschlusssachen verhindert werden kann. Eine Änderung in der Einschätzung der Bedrohungslage kann eine Verschärfung der Ein- und Ausgangskontrollmaßnahmen zur Folge haben, beispielsweise anlässlich des Besuchs hochrangiger Persönlichkeiten.

Kontrollgänge

10. In Sicherheitsbereichen der Kategorien I und II sind außerhalb der normalen Arbeitszeiten Kontrollgänge durchzuführen, um das Eigentum der ESA vor Kenntnisnahme durch Unbefugte, Beschädigung oder Verlust zu schützen. Die Häufigkeit der Kontrollgänge richtet sich nach den örtlichen Gegebenheiten, sie sollten aber in unterschiedlichen Zeitabständen stattfinden.

Sicherheitsbehältnisse und Tresorräume

11. Zur Aufbewahrung von ESA-Verschlusssachen werden drei Arten von Behältnissen verwendet:

– Typ A: Behältnisse, die zur Aufbewahrung von als „ESA STRENG GEHEIM“ eingestuften Verschlusssachen in Sicherheitsbereichen der Kategorie I oder II auf nationaler Ebene zugelassen sind;

– Typ B: Behältnisse, die zur Aufbewahrung von als „ESA GEHEIM“ und „ESA VERTRAULICH“ eingestuften Verschlusssachen in Sicherheitsbereichen der Kategorie I oder II auf nationaler Ebene zugelassen sind;

– Typ C: Büromöbel, die ausschließlich für die Aufbewahrung von als „ESA NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Verschlusssachen geeignet sind.

12. In den in einem Sicherheitsbereich der Kategorie I oder II eingebauten Tresorräumen und in allen Sicherheitsbereichen der Kategorie I, wo als „ESA VERTRAULICH“ und höher eingestufte Verschlusssachen in offenen Regalen aufbewahrt werden oder auf Karten, Plänen usw. sichtbar sind, werden Wände, Böden, Decken und Türen einschließlich der Schlösser von der zuständigen NSA/DSA geprüft, um festzustellen, dass sie einen Schutz bieten, der dem Typ des Sicherheitsbehältnisses entspricht, der für die Aufbewahrung von Verschlusssachen desselben Geheimhaltungsgrades zugelassen ist.

Schlösser

13. Die Schlösser der Sicherheitsbehältnisse und Tresorräume, in denen ESA-Verschlusssachen aufbewahrt werden, müssen folgende Anforderungen erfüllen:
    – Gruppe A: Sie müssen auf nationaler Ebene für Behältnisse vom Typ A zugelassen sein;
    – Gruppe B: Sie müssen auf nationaler Ebene für Behältnisse vom Typ B zugelassen sein;
    – Gruppe C: Sie müssen ausschließlich für Büromöbel vom Typ C geeignet sein.

Kontrolle der Schlüssel und Kombinationen

14. Die Schlüssel von Sicherheitsbehältnissen dürfen nicht aus dem Bürogebäude entfernt werden. Die Kombinationen für Sicherheitsbehältnisse sind von den Personen, die sie kennen müssen, auswendig zu lernen. Damit sie im Notfall benutzt werden können, ist der Standortsicherheitsbeauftragte oder der Leiter der ESA-Niederlassung oder -Anlage für die Aufbewahrung der Ersatzschlüssel und die schriftliche Registrierung aller Kombinationen verantwortlich; letztere sind einzeln in versiegelten, undurchsichtigen Umschlägen aufzubewahren. Die Arbeitsschlüssel, die Ersatzsicherheitsschlüssel und die Kombinationen sind in gesonderten Sicherheitsbehältnissen aufzubewahren. Für diese Schlüssel und Kombinationen ist kein geringerer Sicherheitsschutz vorzusehen als für das Material, zu dem sie den Zugang ermöglichen.
15. Der Kreis der Personen, die die Kombinationen der Sicherheitsbehältnisse kennen, ist so weit wie möglich zu begrenzen. Die Kombinationen sind zu ändern
    a) bei Entgegennahme eines neuen Behältnisses;
    b) bei jedem Benutzerwechsel;
    c) bei tatsächlicher oder vermuteter Kenntnisnahme durch Unbefugte;
    d) vorzugsweise alle sechs Monate und mindestens alle zwölf Monate.

Einbruchmeldeanlagen

16. Kommen zum Schutz von ESA-Verschlusssachen Alarmanlagen, hauseigene Fernsehsysteme und andere elektrische Vorrichtungen zum Einsatz, so ist eine Notstromversorgung vorzusehen, um bei Ausfall der Hauptstromversorgung den ununterbrochenen Betrieb der Anlagen sicherzustellen. Funktionsstörungen dieser Anlagen oder Manipulationen an ihnen müssen ein für das Überwachungspersonal bestimmtes Alarmsignal oder ein anderes verlässliches Signal auslösen.

Zugelassene Ausrüstung

17. Das ESA-Sicherheitsbüro unterhält ein Verzeichnis der zugelassenen Sicherheitsausrüstung, das unter anderem auf den von den NSA/DSA mitgeteilten Informationen beruht. Die Abteilung Standortverwaltung konsultiert über das ESA-Sicherheitsbüro gegebenenfalls die NSA/DSA des Mitgliedstaats, in dem die Hauptverwaltung, Niederlassung oder Anlage der ESA angesiedelt ist, bevor sie derartige Ausrüstungen erwirbt.

Materieller Geheimschutz für Kopier- und Faxgeräte

18. Für Kopier- und Faxgeräte ist im erforderlichen Umfang durch Maßnahmen des materiellen Geheimschutzes dafür zu sorgen, dass sie lediglich von befugten Personen verwendet werden können und dass alle Verschlusssachen einer ordnungsgemäßen Überwachung unterliegen.

SICHT- UND ABHÖRSCHUTZ

Sichtschutz

19. Es sind alle geeigneten Maßnahmen zu treffen, damit bei Tag und bei Nacht gewährleistet ist, dass ESA-Verschlusssachen nicht – auch nicht versehentlich – von Unbefugten eingesehen werden können.

Abhörschutz

20. Die Büroräume oder Bereiche, in denen regelmäßig über als „ESA GEHEIM“ und höher eingestufte Verschlusssachen gesprochen wird, sind bei entsprechendem Risiko gegen Ab- und Mithö-

ren zu schützen. Für die Einschätzung des Risikos ist das ESA-Sicherheitsbüro zuständig, das erforderlichenfalls zuvor die zuständigen NSA/DSA zu Rate zieht.

21. Mobilfunktelefone, private Computer, Aufnahmegeräte, Kameras und andere elektronische Geräte sind in Sicherheitsbereichen oder Hochsicherheitszonen nur mit vorheriger Genehmigung des Leiters des ESA-Sicherheitsbüros zugelassen.
22. Zur Festlegung der Schutzmaßnahmen für mithörgefährdete Bereiche (beispielsweise Schalldämpfung von Wänden, Türen, Böden und Decken, Lautstärkemessung) bzw. abhörgefährdete Bereiche (beispielsweise Suche nach Mikrofonen) kann das ESA-Sicherheitsbüro die zuständige NSA/DSA um Unterstützung durch Sachverständige ersuchen. Die Standortsicherheitsbeauftragten der Hauptverwaltung, Niederlassungen oder Anlagen der ESA können darum ersuchen, dass das ESA-Sicherheitsbüro gegebenenfalls mit Unterstützung durch Sachverständige der zuständigen NSA/DSA technische Kontrollen durchführt.
23. Ebenso können die für die technische Sicherheit zuständigen Sachverständigen der NSA/DSA erforderlichenfalls die Telekommunikationseinrichtungen und die elektrischen oder elektronischen Büromaschinen aller Art, die in den Sitzungen des Geheimhaltungsgrades „ESA GEHEIM“ und höher verwendet werden, auf Ersuchen des Leiters des ESA-Sicherheitsbüros überprüfen. Solche Überprüfungen werden in enger Abstimmung mit der Abteilung Standortverwaltung durchgeführt.

HOCHSICHERHEITSZONEN

24. Bestimmte Bereiche können als Hochsicherheitszonen ausgewiesen werden. Hier findet eine besondere Zutrittskontrolle statt. Diese Zonen bleiben nach einem zugelassenen Verfahren verschlossen, wenn sie nicht besetzt sind, und alle Schlüssel sind als Sicherheitsschlüssel zu behandeln. Diese Zonen unterliegen regelmäßigen Objektschutzkontrollen, die von der Abteilung Standortverwaltung unter der Leitung des ESA-Sicherheitsbüros durchgeführt werden. Diese Kontrollen werden auch durchgeführt, wenn festgestellt oder vermutet wird, dass die Zonen ohne Genehmigung betreten wurden.
25. Es wird eine detaillierte Bestandsaufnahme der Geräte und Möbel vorgenommen. Kein Möbelstück oder Gerät wird in eine dieser Zonen verbracht, bevor es nicht durch Sicherheitspersonal, das für das Aufspüren von Abhörvorrichtungen besonders geschult ist, sorgfältig kontrolliert worden ist. In der Regel sollten in Hochsicherheitszonen möglichst keine Telekommunikationsverbindungen installiert werden.

ABSCHNITT V
ZUGANG ZU ESA-VERSCHLUSSSACHEN

1. Der Zugang zu ESA-Verschlusssachen wird nur Personen gestattet, die Kenntnis von ihnen haben müssen, um die ihnen übertragenen Aufgaben oder Aufträge erfüllen zu können. Der Zugang zu als „ESA STRENG GEHEIM“, „ESA GEHEIM“ und „ESA VERTRAULICH“ eingestuften Verschlusssachen wird nur Personen gestattet, die der entsprechenden Sicherheitsüberprüfung unterzogen worden sind.
2. Das ESA-Sicherheitsbüro erstellt eine Liste der Dienstposten, für die der Zugang zu ESA-Verschlusssachen erforderlich ist. Für die Entscheidung darüber, wer Kenntnis haben muss, sind der Generaldirektor, der Leiter der Hauptverwaltung, Niederlassungen oder Anlagen der ESA und die nationale Stelle, in der die betreffende Person beschäftigt werden soll, entsprechend den Anforderungen der jeweiligen Aufgabe verantwortlich.
3. Für die Sicherheitsüberprüfung von Personen sind die zuständigen Behörden der Mitgliedstaaten nach Maßgabe der anwendbaren Verfahren verantwortlich. Am Ende des Verfahrens wird eine „Sicherheitsunbedenklichkeitsbescheinigung“ ausgestellt, in dem der höchste Geheimhaltungsgrad der ESA-Verschlusssachen, zu denen die überprüfte Person Zugang erhalten darf, und das Ende der Gültigkeitsdauer der Bescheinigung angegeben werden.
4. Beschäftigte der ESA-Auftragnehmer, die in den Infrastruktur- und Unterstützungdiensten in der Hauptverwaltung, den Niederlassungen oder den Anlagen der ESA tätig sind und deren Aufgaben ihnen Zugang zu ESA-Verschlusssachen gewähren können, von denen sie Kenntnis haben müssen, müssen zunächst im Einklang mit den Bestimmungen dieses Abschnitts einer angemessenen Sicherheitsüberprüfung unterzogen werden.
5. Sollen Personen, die nicht nachweislich Kenntnis haben müssen, unter Bedingungen beschäftigt werden, die ihnen Zugang zu ESA-Verschlusssachen gewähren können (z.B. Boten, Sicherheits-,

Wartungs- und Reinigungspersonal, usw.), müssen sie zunächst im Einklang mit den Bestimmungen dieses Abschnitts einer angemessenen Sicherheitsüberprüfung unterzogen werden.

6. Personen, bei denen es sich nicht um Bedienstete oder Sachverständige der ESA oder um Beamte oder sonstige Bedienstete der Mitgliedstaaten handelt, mit denen möglicherweise ESA-Verschlusssachen erörtert werden müssen oder die möglicherweise Einblick in diese erhalten müssen, müssen einer Sicherheitsüberprüfung in Bezug auf Verschlusssachen unterzogen und über ihre Verantwortung für die Sicherheit belehrt worden sein.
7. Personen, die Zugang zu ESA-Verschlusssachen haben, werden nach Abschnitt X von den Folgen der Verletzung der Sicherheit und der Kenntnisnahme von ESA-Verschlusssachen durch Unbefugte in Kenntnis gesetzt.

BESONDERE VORSCHRIFTEN FÜR DEN ZUGANG ZU ALS „ESA STRENG GEHEIM“ EINGESTUFTEN VERSCHLUSSSACHEN

8. Alle Personen, die Zugang zu als „ESA STRENG GEHEIM“ eingestuften Verschlusssachen benötigen, sind von ihren Abteilungsleitern zu benennen und ihre Namen in das einschlägige „ESA STRENG GEHEIM“-Register einzutragen.
9. Bevor diesen Personen der Zugang zu als „ESA STRENG GEHEIM“ eingestuften Verschlusssachen gewährt wird, müssen sie eine Urkunde des Inhalts unterzeichnen, dass sie über die Sicherheitsverfahren der ESA belehrt worden sind und sich ihrer besonderen Verantwortung für den Schutz von als „ESA STRENG GEHEIM“ eingestuften Verschlusssachen und der Folgen, die in den ESA-Vorschriften und den einzelstaatlichen Rechts- und Verwaltungsvorschriften für den Fall vorgesehen sind, dass Verschlusssachen durch Vorsatz oder durch Fahrlässigkeit in die Hände Unbefugter gelangen, vollständig bewusst sind.
10. Müssen Personen in Sitzungen Zugang zu als „ESA STRENG GEHEIM“ eingestuften Verschlusssachen erhalten, so teilt der Sicherheitsbeauftragte der Dienststelle oder des Gremiums, bei der bzw. dem die Betreffenden beschäftigt sind, der die Sitzung veranstaltenden Stelle mit, dass die betreffenden Personen einer angemessenen Sicherheitsüberprüfung unterzogen wurden.
11. Die Namen aller Personen, die nicht mehr für Aufgaben eingesetzt werden, bei denen sie Zugang zu als „ESA STRENG GEHEIM“ eingestuften Verschlusssachen haben müssen, werden aus dem “ESA STRENG GEHEIM”-Verzeichnis gestrichen. Ferner werden diese Personen erneut über ihre besondere Verantwortung für den Schutz von als “ESA STRENG GEHEIM” eingestuften Verschlusssachen belehrt. Sie haben ferner eine Erklärung zu unterzeichnen, wonach sie ihre Kenntnisse über als “ESA STRENG GEHEIM” eingestufte Verschlusssachen weder verwenden noch weitergeben werden.

BESONDERE VORSCHRIFTEN FÜR DEN ZUGANG ZU ALS „ESA GEHEIM“ UND „ESA VERTRAULICH“ EINGESTUFTEN VERSCHLUSSSACHEN

12. Alle Personen, die Zugang zu als „ESA GEHEIM“ oder „ESA VERTRAULICH“ eingestuften Verschlusssachen benötigen, müssen über die entsprechenden Sicherheitsregelungen unterrichtet werden und sich der Folgen fahrlässigen Handelns bewusst sein.
13. Wenn Personen in Sitzungen Zugang zu als „ESA GEHEIM“ oder „ESA VERTRAULICH“ eingestuften Verschlusssachen erhalten, so teilt der Sicherheitsbeauftragte der Stelle, bei der die Betreffenden beschäftigt sind, der die Sitzung veranstaltenden Stelle mit, dass die betreffenden Personen die entsprechende Ermächtigung besitzen.

BESONDERE VORSCHRIFTEN FÜR DEN ZUGANG ZU ALS „ESA NUR FÜR DEN DIENSTGEBRAUCH“ EINGESTUFTEN VERSCHLUSSSACHEN

14. Alle Personen, die Zugang zu als „ESA NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Verschlusssachen haben, werden auf diese Sicherheitsvorschriften, ihre Verantwortung für den Schutz dieser Verschlusssachen und die Folgen fahrlässigen Handelns aufmerksam gemacht.

WEITERGABE

15. Wird eine Person von einem Dienstposten, der mit der Arbeit mit ESA-Verschlusssachen verbunden ist, wegversetzt, so achtet die Registratur darauf, dass die betreffenden Verschlusssachen ordnungsgemäß von dem ausscheidenden an den eintretenden Bediensteten weitergegeben werden.

BESONDERE ANWEISUNGEN

16. Personen, die mit ESA-Verschlusssachen arbeiten müssen, sollten bei Aufnahme ihrer Tätigkeit und danach in regelmäßigen Abständen auf folgendes hingewiesen werden:

    a) die mögliche Gefährdung der Sicherheit durch indiskrete Gespräche;

b) die in den Beziehungen zur Presse und zu Vertretern besonderer Interessengruppen zu treffenden Vorsichtsmaßnahmen;

c) die Bedrohung für ESA-Verschlusssachen und ihre geheimhaltungsbedürftigen Tätigkeiten unter anderem durch gegen die ESA und ihre Mitgliedstaaten gerichtete Spionage von Nachrichtendiensten oder privatwirtschaftlichen Unternehmen, Sabotage oder Terrorismus oder durch die Aktionen subversiver und/oder krimineller Gruppen;

d) die Verpflichtung, die zuständigen Sicherheitsbehörden unverzüglich über jeden Annäherungsversuch oder jede Handlungsweise, bei denen ein Verdacht auf Spionage entsteht, sowie über alle ungewöhnlichen Umstände in bezug auf die Sicherheit zu unterrichten.

17. Alle Personen, die gewöhnlich häufige Kontakte mit Vertretern von Ländern haben, deren Nachrichtendienste in bezug auf ESA-Verschlusssachen und ihre geheimhaltungsbedürftigen Tätigkeiten gegen die ESA und ihre Mitgliedstaaten arbeiten könnten, sind über die Techniken zu belehren, von denen bekannt ist, dass sich die einzelnen Nachrichtendienste ihrer bedienen.
18. Es bestehen keine Sicherheitsregelungen der ESA für private Reisen der zum Zugang zu ESA-Verschlusssachen ermächtigten Personen nach irgendeinem Zielland. Die zuständigen Sicherheitsbehörden werden jedoch die Bediensteten, für die sie zuständig sind, über Reiseregelungen unterrichten, denen sie möglicherweise unterliegen. Die Sicherheitsbeauftragten sind dafür verantwortlich, für die Betreffenden Sitzungen zur Auffrischung der Kenntnisse über diese besonderen Anweisungen zu veranstalten.

ABSCHNITT VI

VERFAHREN FÜR DIE SICHERHEITSÜBERPRÜFUNG VON BEDIENSTETEN UND SACHVERSTÄNDIGEN DER ESA

1. Nur Bedienstete und Sachverständige der ESA, die aufgrund ihrer Aufgabenbereiche und dienstlicher Erfordernisse von ESA-Verschlusssachen Kenntnis nehmen müssen oder sie zu bearbeiten haben, erhalten Zugang zu diesen Verschlusssachen unter der Voraussetzung, dass sie von der zuständigen nationalen Behörde einer angemessenen Sicherheitsüberprüfung unterzogen worden sind.
2. Um Zugang zu den als „ESA STRENG GEHEIM“, „ESA GEHEIM“ und „ESA VERTRAULICH“ eingestuften Verschlusssachen zu erhalten, müssen die Bediensteten und Sachverständigen der ESA im Besitz einer ESA-Sicherheitsunbedenklichkeitsbescheinigung (PSC) sein, die von den zuständigen Behörden der Mitgliedstaaten (nationale Sicherheitsbehörde oder entsprechende nationale Behörde) erteilt wird.
3. Die PSC ist für die Einstufung „ESA STRENG GEHEIM“ höchstens fünf Jahre und für die Einstufungen „ESA GEHEIM“ und „ESA VERTRAULICH“ höchstens zehn Jahre gültig. Die auf der Grundlage dieser PSC erteilte Zugangsermächtigung erlischt, wenn die Aufgaben, für die sie erteilt wurde, nicht mehr wahrgenommen werden.
4. Die Sicherheitsüberprüfung wird unter Mitwirkung des betreffenden Bediensteten oder Sachverständigen der ESA auf Ersuchen des Generaldirektors von den zuständigen nationalen Behörden desjenigen Mitgliedstaats vorgenommen, dessen Staatsangehörigkeit der Bedienstete oder Sachverständige besitzt. Hat der Bedienstete oder Sachverständige der ESA seinen Wohnsitz in einem anderen Mitgliedstaat, so können die betreffenden nationalen Behörden sich die Mitwirkung der Behörden des Wohnsitzstaats sichern.
5. Der betreffende Bedienstete oder Sachverständige der ESA hat im Hinblick auf die Sicherheitsüberprüfung eine Sicherheitserklärung auszufüllen und zu bestätigen, dass er versteht, dass eine Verletzung der Sicherheit der ESA die Aufhebung seiner ESA-Immunität zur Folge haben könnte.
6. Der Generaldirektor benennt in seinem Ersuchen die Art und den Geheimhaltungsgrad der Informationen, zu denen der betreffende Bedienstete oder Sachverständige der ESA Zugang erhalten soll, damit die NSA/DSA oder andere zuständige nationale Behörden das Sicherheitsüberprüfungsverfahren durchführen können.
7. Für den gesamten Ablauf und die Ergebnisse des Sicherheitsüberprüfungsverfahrens gelten die einschlägigen Vorschriften und Regelungen des betreffenden Mitgliedstaats, einschließlich der Vorschriften und Regelungen für etwaige Rechtsbehelfe.
8. Erteilt die zuständige NSA/DSA eines Mitgliedstaats eine Sicherheitsunbedenklichkeitsbescheinigung, kann der Generaldirektor den betreffenden Bediensteten oder Sachver-

ständigen der ESA zum Zugang zu Verschlusssachen ermächtigen, wenn dieser Bedienstete oder Sachverständige von ihnen Kenntnis haben muss.

9. Lehnt die NSA/DSA die Erteilung einer Sicherheitsunbedenklichkeitsbescheinigung ab, so teilt der Generaldirektor dies dem betreffenden Bediensteten oder Sachverständigen der ESA mit, der darum bitten kann, vom Generaldirektor gehört zu werden. Der Generaldirektor sucht bei der zuständigen nationalen Behörde um alle weiteren Auskünfte nach, die diese nach Maßgabe ihrer nationalen Vorschriften und Regelungen zu geben vermag. Bei Bestätigung der Ablehnung durch die NSA/DSA wird die Zugangsermächtigung nicht erteilt.
10. Jeder Bedienstete und jeder Sachverständige der ESA, dem eine PSC erteilt wurde, erhält zum Zeitpunkt der Ermächtigung und danach in regelmäßigen Abständen die gebotenen Anweisungen zum Schutz der Verschlusssachen und zu den Verfahren zur Sicherstellung dieses Schutzes. Diese Personen unterzeichnen eine Erklärung, mit der sie den Erhalt dieser Anweisungen bestätigen und sich zu ihrer Einhaltung verpflichten.
11. Die Zugangsermächtigung zu ESA-Verschlusssachen wird vom Generaldirektor entzogen, wenn die zuständige NSA/DSA die Sicherheitsunbedenklichkeitsbescheinigung entzieht. Die Entzugsverfügung wird dem betreffenden Bediensteten oder Sachverständigen der ESA mitgeteilt, der darum bitten kann, vom Generaldirektor gehört zu werden. Der Generaldirektor kann bei der zuständigen nationalen Behörde um alle weiteren Auskünfte nachsuchen, die diese nach Maßgabe ihrer nationalen Vorschriften und Regelungen zu geben vermag.
12. Der Generaldirektor ergreift alle erforderlichen Maßnahmen für die Durchführung dieses Abschnitts, insbesondere hinsichtlich der Regelung für den Zugang zum Verzeichnis der sicherheitsüberprüften Bediensteten oder Sachverständigen der ESA.
13. Ausnahmsweise kann der Generaldirektor mit der schriftlichen Zustimmung der NSA/DSA oder einer anderen zuständigen nationalen Behörde einem Bediensteten der ESA für höchstens sechs Monate eine einstweilige Ermächtigung zum Zugang zu als „ESA GEHEIM“ oder niedriger eingestuften Verschlusssachen erteilen, bis ihm die Ergebnisse der Sicherheitsüberprüfung vorliegen.
14. Die so erteilten vorläufigen und befristeten Ermächtigungen berechtigen nicht zum Zugang zu als „ESA STRENG GEHEIM“ eingestuften Verschlusssachen; dieser Zugang wird auf die Bediensteten der ESA beschränkt, denen eine PSC für diese Einstufung erteilt wurde. Bis die Ergebnisse der Sicherheitsüberprüfung vorliegen, können die Bediensteten der ESA, die die Ermächtigungsstufe „ESA STRENG GEHEIM“ erhalten sollen, vorläufig und befristet zum Zugang zu als „ESA GEHEIM“ oder niedriger eingestuften Verschlusssachen ermächtigt werden.

ABSCHNITT VII

HERSTELLUNG, VERTEILUNG, ÜBERMITTLUNG, AUFBEWAHRUNG UND VERNICHTUNG VON ESA-VERSCHLUSSSACHEN

Allgemeine Bestimmungen

Dieser Abschnitt bestimmt die Maßnahmen, die bei der Herstellung, Verteilung, Übermittlung, Aufbewahrung und Vernichtung von als ESA-Verschlusssachen eingestuften Dokumenten zu treffen sind. Er ist als Grundlage heranzuziehen, wenn diese Maßnahmen für sonstiges als ESA-Verschlusssache eingestuftes Material unter Berücksichtigung der Art des jeweils betroffenen Materials in jedem Einzelfall angepasst werden.

Kapitel I

Herstellung und Verteilung von ESA-Verschlusssachen

HERSTELLUNG

1. Die ESA-Geheimhaltungsgrade und sonstigen Kennzeichnungen sind in der in Abschnitt II angegebenen Weise oben und unten in der Mitte auf jeder Seite anzubringen, wobei jede Seite zu nummerieren ist. Auf jeder ESA-Verschlusssache sind ein Aktenzeichen und ein Datum anzugeben. Im Falle von Dokumenten der Geheimhaltungsgrade „ESA STRENG GEHEIM“ und „ESA GEHEIM“ muss das Aktenzeichen auf jeder Seite erscheinen. Werden sie in mehreren Ausfertigungen verteilt, so erhält jede Ausfertigung eine eigene Nummer, die auf der ersten Seite zusammen mit der Gesamtzahl der Seiten anzugeben ist. Alle Anhänge und Anlagen sind auf der ersten Seite von Dokumenten aufzulisten, die als „ESA VERTRAULICH“ oder höher eingestuft werden.

2. Dokumente, die als „ESA VERTRAULICH“ oder höher eingestuft werden, dürfen nur von Personen maschinegeschrieben, übersetzt, archiviert, fotokopiert und auf Magnetband oder Mikrofiche gespeichert werden, die eine zumindest dem Geheimhaltungsgrad des betreffenden Dokuments entsprechende Zugangsermächtigung zu ESA-Verschlusssachen haben.

Abschnitt XI enthält die Vorschriften für die Erstellung von Verschlusssachen mit Hilfe eines Computers.

VERTEILUNG

3. ESA-Verschlusssachen dürfen nur an Personen verteilt werden, für die deren Kenntnis nötig ist und die in entsprechender Weise sicherheitsüberprüft worden sind. Der Urheber bestimmt die Empfänger der erstmaligen Verteilung.
4. Dokumente des Geheimhaltungsgrades „ESA STRENG GEHEIM“ werden über „ESA STRENG GEHEIM“-Registraturen verteilt (siehe Abschnitt VIII). Im Falle von Mitteilungen, die als „ESA STRENG GEHEIM“ eingestuft sind, kann die zuständige Registratur dem Leiter des Kommunikationszentrums gestatten, die in der Liste der Empfänger angegebene Anzahl von Ausfertigungen zu erstellen.
5. Als „ESA GEHEIM“ eingestufte Dokumente werden über Registraturen verteilt. Sie können vom Erstempfänger an weitere Empfänger, für die deren Kenntnis nötig ist, weitergegeben werden. Die Stellen, von denen die Verschlusssachen stammen, können allerdings von ihnen gewünschte Einschränkungen bei der Verteilung mitteilen. In diesem Fall dürfen die Empfänger die Dokumente nur mit der Genehmigung der Stellen, von denen sie stammen, weitergeben.
6. Ein- und Ausgang jedes als „ESA VERTRAULICH“ eingestuften Dokuments sind von der Registratur der jeweiligen Einrichtung zu verzeichnen. Die Angaben, die hierbei zu erfassen sind (Aktenzeichen, Datum und gegebenenfalls Nummer der Ausfertigung) müssen eine Identifizierung des Dokuments ermöglichen und sind in einem Dienstbuch oder in einem besonders geschützten Computermedium festzuhalten.

Kapitel II
Übermittlung von ESA-Verschlusssachen

VERSAND

7. Als „ESA VERTRAULICH“ oder höher eingestufte Dokumente sind in einem doppelten, widerstandsfähigen und undurchsichtigen Umschlag zu übermitteln. Auf dem inneren Umschlag sind der entsprechende ESA-Geheimhaltungsgrad sowie möglichst die vollständige Amtsbezeichnung und Anschrift des Empfängers anzugeben.
8. Nur der Registraturkontrollbeauftragte oder sein Stellvertreter darf den inneren Umschlag öffnen und den Empfang der übermittelten Verschlusssachen bestätigen, es sei denn, der Umschlag ist ausdrücklich an einen bestimmten Empfänger gerichtet. In diesem Fall vermerkt die zuständige Registratur den Eingang des Umschlags, und nur der genannte Empfänger darf den inneren Umschlag öffnen und den Empfang der darin enthaltenen Verschlusssachen bestätigen.
9. In dem inneren Umschlag ist eine Empfangsbestätigung beizulegen. In dieser Bestätigung, die nicht als Verschlusssache eingestuft wird, sind Aktenzeichen, Datum und die Nummer der Ausfertigung der Verschlusssache, niemals jedoch deren Betreff, anzugeben.
10. Der innere Umschlag wird in einen Außenumschlag gelegt, der für Empfangszwecke eine Versandnummer erhält. Der Geheimhaltungsgrad darf unter keinen Umständen auf dem Außenumschlag erscheinen.
11. Bei als „ESA VERTRAULICH“ oder höher eingestuften Dokumenten ist Kurieren und Boten eine Empfangsbestätigung auszustellen, auf der die Versandnummern der übermittelten Versandstücke angegeben sind.

ÜBERMITTLUNG INNERHALB EINES GEBÄUDES ODER GEBÄUDEKOMPLEXES

12. Innerhalb eines bestimmten Gebäudes oder Gebäudekomplexes dürfen als Verschlusssachen eingestufte Dokumente in einem versiegelten Umschlag, der nur den Namen des Empfängers trägt, befördert werden, sofern die Beförderung durch eine für den betreffenden Geheimhaltungsgrad ermächtigte Person erfolgt.

ÜBERMITTLUNG VON ESA-DOKUMENTEN INNERHALB EIN UND DESSELBEN LANDES

13. Innerhalb ein und desselben Landes sollten „ESA STRENG GEHEIM“-Dokumente nur durch offizielle Kuriere oder durch Personen übermittelt werden, die eine Zugangsermächtigung zu als „ESA STRENG GEHEIM“ eingestuften Verschlusssachen haben.

14. Wird zur Übermittlung eines als „ESA STRENG GEHEIM“ eingestuften Dokuments an einen Empfänger außerhalb desselben Gebäudes oder Gebäudekomplexes ein offizieller Kurier verwendet, so sind die Bestimmungen über den Versand und die Empfangsbestätigung in diesem Kapitel einzuhalten. Die Zustelldienste sind personell so auszustatten, dass gewährleistet ist, dass sich Versandstücke mit als „ESA STRENG GEHEIM“ eingestuften Dokumenten jederzeit unter der direkten Aufsicht eines Verantwortlichen befinden.
15. In Ausnahmefällen können befugte Personen, die nicht offizielle Kuriere sind, als „ESA STRENG GEHEIM“ eingestufte Dokumente außerhalb des Gebäudes oder Gebäudekomplexes zur Benutzung vor Ort anlässlich von Sitzungen oder Erörterungen mitnehmen, vorausgesetzt, dass
    a) die betreffende Person zum Zugang zu diesen als „ESA STRENG GEHEIM“ eingestuften Dokumenten ermächtigt ist;
    b) die Form der Beförderung den einzelstaatlichen Vorschriften für die Übermittlung einzelstaatlicher Dokumente des Geheimhaltungsgrades „STRENG GEHEIM“ entspricht;
    c) die betreffende Person die Dokumente des Geheimhaltungsgrades „ESA STRENG GEHEIM“ unter keinen Umständen unbeaufsichtigt lässt;
    d) Vorkehrungen getroffen werden, damit die Liste der Dokumente, die mitgenommen werden, in der „ESA STRENG GEHEIM”-Registratur verwahrt, in einem Dienstbuch vermerkt und bei Rückkehr anhand dieses Eintrags kontrolliert wird.
16. Innerhalb ein und desselben Landes dürfen als „ESA GEHEIM“ oder „ESA VERTRAULICH“ eingestufte Dokumente entweder mit der Post, wenn eine derartige Übermittlung nach den einzelstaatlichen Regelungen gestattet ist und mit den hier vorliegenden Vorschriften in Einklang steht, oder durch offizielle Kuriere oder durch Personen übermittelt werden, die zum Zugang zu ESA-Verschlusssachen ermächtigt sind.
17. Jeder Mitgliedstaat und die ESA sollten auf diesen Vorschriften beruhende Weisungen für das Personal ausarbeiten, das ESA-Verschlusssachen befördert. Es sollte vorgeschrieben werden, dass Personen, die Verschlusssachen befördern, diese Weisungen lesen und unterzeichnen. In den Weisungen sollte insbesondere deutlich gemacht werden, dass Dokumente unter keinen Umständen
    a) von der sie befördernden Person aus den Händen gegeben werden dürfen, es sei denn, sie sind entsprechend den Bestimmungen in Abschnitt IV in sicherem Gewahrsam;
    b) in öffentlichen Transportmitteln oder Privatfahrzeugen oder an Orten wie Restaurants oder Hotels unbeaufsichtigt bleiben dürfen. Sie dürfen nicht in Hotelsafes verwahrt werden oder unbeaufsichtigt in Hotelzimmern zurückbleiben;
    c) in der Öffentlichkeit (beispielsweise in Flugzeugen oder Zügen) gelesen werden dürfen.

BEFÖRDERUNG VOM HOHEITSGEBIET EINES MITGLIEDSTAATES IN DAS HOHEITSGEBIET EINES ANDEREN

18. Als „ESA VERTRAULICH“ oder höher eingestuftes Material sollte durch diplomatische Kuriere von einem Mitgliedstaat in einen anderen befördert werden.
19. Eine persönliche Beförderung von als „ESA GEHEIM“ oder „ESA VERTRAULICH“ eingestuftem Material kann jedoch gestattet werden, wenn durch die für die Beförderung geltenden Vorschriften gewährleistet wird, dass das Material nicht in die Hände Unbefugter fallen kann.
20. Die NSA/DSA können eine persönliche Beförderung gestatten, wenn keine diplomatischen Kuriere zur Verfügung stehen oder der Rückgriff auf derartige Kuriere zu einer Verzögerung führen würde, die sich nachteilig auf Tätigkeiten der ESA auswirken könnte, und wenn das Material vom Empfänger dringend benötigt wird. Jeder Mitgliedstaat sollte Anweisungen über die zwischenstaatliche persönliche Beförderung von Material des Geheimhaltungsgrades „ESA GEHEIM“ oder geringer durch Personen, die keine diplomatischen Kuriere sind, ausarbeiten. In diesen Anweisungen sollte vorgesehen werden, dass
    a) die Person, die das Material mit sich führt, über die entsprechende, von den Mitgliedstaaten ausgesprochene Zugangsermächtigung verfügen muss;
    b) sämtliches auf diese Weise befördertes Material in der zuständigen Dienststelle oder der zuständigen Registratur verzeichnet sein muss;
    c) Versandstücke oder Taschen, die ESA-Material enthalten, mit einem Dienstsiegel zu versehen sind, um Zollkontrollen zu vermeiden oder diesen vorzubeugen, sowie mit Etiketten zu ihrer Erkennung und mit Weisungen für den Finder;

d) die Person, die das Material mit sich führt, einen Kurierausweis und/oder einen Dienstreiseauftrag mitführen muss, die von allen ESA-Mitgliedstaaten anerkannt sind und diese Person ermächtigen, das betreffende Versandstück in der beschriebenen Weise zu befördern;

e) bei Überlandreisen die Grenze keines Staates, der nicht Mitglied der ESA ist, überschritten oder dieser Staat durchfahren werden darf, es sei denn, dass der Staat, der die Beförderung vornimmt, über eine besondere Garantie seitens dieses Staates verfügt;

f) die Reiseplanung der Person, die das Material mit sich führt, im Hinblick auf Bestimmungsorte, Fahrtrouten und Beförderungsmittel mit den ESA-Vorschriften oder mit einzelstaatlichen Vorschriften, falls diese in dieser Hinsicht strenger sind, in Einklang stehen muss;

g) das Material von der Person, die es mit sich führt, nicht aus der Hand gegeben werden darf, außer wenn es nach den Bestimmungen des Abschnitts IV über sicheren Gewahrsam verwahrt ist;

h) das Material nicht in öffentlichen Transportmitteln oder Privatfahrzeugen oder an Orten wie Restaurants oder Hotels unbeaufsichtigt bleiben darf. Es darf nicht in Hotelsafes verwahrt werden oder unbeaufsichtigt in Hotelzimmern zurückbleiben;

i) Dokumente, falls solche Bestandteil des beförderten Materials sind, nicht in der Öffentlichkeit (beispielsweise in Flugzeugen, Zügen usw.) gelesen werden dürfen.

Die mit der Beförderung der Verschlusssachen beauftragte Person muss Geheimschutzvorschriften lesen und unterzeichnen, die mindestens die vorstehenden Weisungen sowie Verfahren enthalten, die im Notfall oder für den Fall zu beachten sind, dass das Versandstück mit den Verschlusssachen von Zollbeamten oder Sicherheitsbeamten auf einem Flughafen kontrolliert werden soll.

ÜBERMITTLUNG VON DOKUMENTEN DES GEHEIMHALTUNGSGRADES „ESA NUR FÜR DEN DIENSTGEBRAUCH“

21. Als „ESA NUR FÜR DEN DIENSTGEBRAUCH“ eingestufte Verschlusssachen werden in der Regel in einem Einzelumschlag ohne Angabe des Geheimhaltungsgrades übermittelt durch

a) die normale Post oder soweit zweckmäßig als Einschreiben;

b) kommerzielle Kurierdienste;

c) persönliche Beförderung über Bedienstete ohne förmlichen Kurierauftrag. Während der Reise müssen die Verschlusssachen in ständigem persönlichem Gewahrsam bleiben und dürfen nicht unbeaufsichtigt in Hotelzimmern oder Fahrzeugen zurückbleiben und in der Öffentlichkeit gelesen werden.

SICHERHEIT DER KURIERE

22. Alle Kuriere und Boten, die mit der Beförderung von „ESA GEHEIM“- und „ESA VERTRAULICH“-Dokumenten beauftragt werden, müssen entsprechend sicherheitsermächtigt sein.

Kapitel III

Übermittlung über informationstechnische und Informationssysteme

23. Mit den Maßnahmen für die Kommunikationssicherheit soll die sichere Übermittlung von ESA-Verschlusssachen gewährleistet werden. Die für die Übermittlung dieser ESA-Verschlusssachen geltenden Vorschriften sind in Abschnitt XI festgelegt.

24. Als „ESA VERTRAULICH“ oder „ESA GEHEIM“ eingestufte Informationen dürfen nur von zugelassenen Kommunikationszentren und -netzen und/oder Terminals bzw. über entsprechende Systeme übermittelt werden.

Kapitel IV

Zusätzliche Kopien und Übersetzungen von beziehungsweise Auszüge aus ESA-Verschlusssachen

25. Das Kopieren oder die Übersetzung von „ESA STRENG GEHEIM“-Dokumenten kann ausschließlich der Urheber gestatten.

26. Fordern Personen, die nicht über eine „ESA STRENG GEHEIM“-Sicherheitsermächtigung verfügen, Informationen an, die zwar in einem „ESA STRENG GEHEIM“-Dokument enthalten, aber nicht als solche eingestuft sind, so kann der Leiter der „ESA STRENG GEHEIM“-Registratur ermächtigt werden, die notwendige Anzahl von Auszügen aus diesem Dokument aus-

zuhändigen. Gleichzeitig ergreift er die erforderlichen Maßnahmen, um sicherzustellen, dass diese Auszüge einen angemessenen Geheimhaltungsgrad erhalten.

27. Als „ESA GEHEIM“ und niedriger eingestufte Dokumente können vom Empfänger unter Einhaltung der einzelstaatlichen Sicherheitsvorschriften und unter strikter Befolgung des Grundsatzes „Kenntnis nur wenn nötig“ vervielfältigt und übersetzt werden. Die für das Originaldokument geltenden Sicherheitsvorschriften finden auch auf Vervielfältigungen und/oder Übersetzungen dieses Dokuments Anwendung.

Kapitel V

Bestandsaufnahme, Prüfung, Archivierung und Vernichtung von ESA-Verschlusssachen

BESTANDSAUFNAHME UND PRÜFUNG

28. Alljährlich führt jede „ESA STRENG GEHEIM“-Registratur im Sinne des Abschnitts VIII gemäß den Vorschriften des Abschnitts VIII Nummern 9 bis 11 eine detaillierte Bestandsaufnahme der „ESA STRENG GEHEIM“-Dokumente durch. ESA-Verschlusssachen unterhalb des Geheimhaltungsgrades „ESA STRENG GEHEIM“ werden gemäß den einzelstaatlichen Leitlinien oder im Falle der ESA gemäß den Anweisungen des Generaldirektors einer internen Prüfung unterzogen.

Hierbei soll ermittelt werden, ob nach Auffassung der Verwahrer

a) bestimmte Dokumente heruntergestuft werden können oder ihr Geheimhaltungsgrad aufgehoben werden kann,

b) Dokumente vernichtet werden sollten.

ARCHIVIERUNG VON ESA-VERSCHLUSSSACHEN

29. ESA-Aufzeichnungen und -Archive sind, unabhängig von ihrem Geheimhaltungsgrad, Bestandteil des Eigentums, der Ressourcen und der Vermögenswerte der ESA und müssen entsprechend behandelt werden. Die Archivierung von Verschlusssachen muss mit der Politik und den Verfahren der ESA für die Behandlung von Aufzeichnungen und Archiven im Einklang stehen.

30. Um Archivierungsprobleme möglichst gering zu halten, ist es den Kontrollbeauftragten aller Registraturen gestattet, in Absprache mit dem ESA-Archivar „ESA GEHEIM“-, „ESA VERTRAULICH“- und „ESA NUR FÜR DEN DIENSTGEBRAUCH“-Dokumente auf Mikrofilm aufzunehmen oder auf andere Weise auf magnetischen oder optischen Datenträgern zu Archivzwecken zu speichern, vorausgesetzt

a) das Mikrofilm-Speicherverfahren wird von Personen durchgeführt, die über eine Sicherheitsermächtigung für den dem Dokument entsprechenden Geheimhaltungsgrad verfügen;

b) für den Mikrofilm/Datenträger wird die gleiche Sicherheit gewährleistet wie für die Originaldokumente;

c) die Filmrollen oder sonstigen Träger enthalten nur Dokumente der gleichen „ESA GEHEIM“-, „ESA VERTRAULICH“- oder „ESA NUR FÜR DEN DIENSTGEBRAUCH“-Einstufung;

d) das Mikrofilmen/die Speicherung eines „ESA GEHEIM“-Dokuments wird in dem für die jährliche Bestandsaufnahme verwendeten Register deutlich kenntlich gemacht;

e) die ESA-Originaldokumente, die auf Mikrofilm aufgenommen oder in anderer Weise gespeichert sind, werden gemäß den Vorschriften der Nummern 33 bis 37 vernichtet.

31. Bedienstete oder Sachverständige der ESA müssen bei ihrem Ausscheiden aus der ESA oder vor ihrer Versetzung in eine andere Abteilung oder Einrichtung alle in ihrem Gewahrsam befindlichen Verschlusssachen gemäß Abschnitt V Nummer 14 über die entsprechende Registratur übergeben.

32. Diese Vorschriften gelten auch für alle anderen von der NSA/DSA zugelassenen Speichermedien wie elektromagnetische Träger und optische Speicherplatten.

ROUTINEMÄSSIGE VERNICHTUNG VON ESA-VERSCHLUSSSACHEN

33. Um eine unnötige Anhäufung von ESA-Verschlusssachen zu vermeiden, werden die nach Auffassung der aufbewahrenden Direktion bzw. des Leiters der aufbewahrenden Abteilung inhaltlich überholten Dokumente – mit Ausnahme derjenigen mit langfristigem Wert, die als solche in den ESA-Archiven behandelt werden (siehe die vorangehenden Bestimmungen über die Archivierung) – oder überzähligen Dokumente entsprechend ihrem Geheimhaltungsgrad vernichtet.

34. „ESA STRENG GEHEIM“-Dokumente werden auf folgende Weise vernichtet:

a) „ESA STRENG GEHEIM“-Dokumente werden nur von der für diese Dokumente zuständigen Zentralregistratur vernichtet. Jedes der Vernichtung zugeführte Dokument wird auf einer Ver-

nichtungsbescheinigung eingetragen, die vom „ESA STRENG GEHEIM“-Kontrollbeauftragten und von dem der Vernichtung als Zeuge beiwohnenden Bediensteten, der über die betreffende Sicherheitsermächtigung verfügt, zu unterzeichnen ist. Der Vorgang wird im Dienstbuch festgehalten.

b) Die Registratur bewahrt die Vernichtungsbescheinigungen zusammen mit den Verteilungsunterlagen zehn Jahre lang auf. Dem Urheber oder der zuständigen Zentralregistratur werden Kopien nur zugesandt, wenn dies ausdrücklich verlangt wird.

c) „ESA STRENG GEHEIM“-Dokumente einschließlich des bei ihrer Herstellung angefallenen und als Verschlusssache zu behandelnden Abfalls wie fehlerhafte Kopien, Arbeitsvorlagen, maschinegeschriebene Aufzeichnungen und Disketten werden unter der Aufsicht eines „ESA STRENG GEHEIM“-Registraturkontrollbeauftragten durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so vernichtet, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann.

35. „ESA GEHEIM“-Dokumente werden mittels eines der in Nummer 34 Buchstabe c genannten Verfahren unter der Aufsicht einer Person, die über die betreffende Sicherheitsermächtigung verfügt, von der für diese Dokumente zuständigen Registratur vernichtet. Vernichtete „ESA GEHEIM“-Dokumente werden auf einer unterzeichneten Vernichtungsbescheinigung eingetragen, die von der Registratur zusammen mit den Verteilungsunterlagen mindestens drei Jahre lang aufbewahrt wird.

36. „ESA VERTRAULICH“-Dokumente werden mittels eines der in Nummer 34 Buchstabe c genannten Verfahren unter der Aufsicht einer Person, die über die betreffende Sicherheitsermächtigung verfügt, von der für diese Dokumente zuständigen Registratur vernichtet. Ihre Vernichtung wird gemäß den einzelstaatlichen Vorschriften oder im Falle der ESA gemäß den Anweisungen des Generaldirektors registriert.

37. „ESA NUR FÜR DEN DIENSTGEBRAUCH“-Dokumente werden gemäß den einzelstaatlichen Vorschriften oder im Falle der ESA gemäß den Anweisungen des Generaldirektors vernichtet.

VERNICHTUNG IM NOTFALL

38. Das ESA-Sicherheitsbüro und die Mitgliedstaaten arbeiten unter Berücksichtigung der örtlichen Gegebenheiten Pläne zum Schutz von ESA-Verschlusssachen im Krisenfall aus, die, falls erforderlich, auch Pläne für eine Vernichtung oder Auslagerung der ESA-Verschlusssachen im Notfall umfassen; sie erteilen die Anweisungen, die sie für notwendig erachten, damit ESA-Verschlusssachen nicht in unbefugte Hände gelangen.

39. Regelungen zum Schutz und/oder zur Vernichtung von als „ESA GEHEIM“ und „ESA VERTRAULICH“ eingestuften Verschlusssachen im Krisenfall dürfen auf keinen Fall den Schutz oder die Vernichtung von „ESA STRENG GEHEIM“-Materialien, einschließlich der Verschlüsselungseinrichtungen, beeinträchtigen, deren Behandlung Vorrang vor allen anderen Aufgaben hat. Die für den Schutz und die Vernichtung der Verschlüsselungseinrichtungen im Notfall vorzusehenden Maßnahmen sind durch Ad-hoc-Anweisungen zu regeln.
Die Anweisungen sind an Ort und Stelle in einem versiegelten Umschlag zu hinterlegen. Es müssen Vorrichtungen/Werkzeuge für die Vernichtung vorhanden sein.

Kapitel VI

Besondere Vorschriften für Dokumente, die für den ESA-Rat bestimmt sind

40. Innerhalb der ESA-Hauptverwaltung verfolgt ein „Verschlusssachenbüro“ die Behandlung der als „ESA GEHEIM“ und „ESA VERTRAULICH“ eingestuften Informationen, wenn sie Gegenstand von Ratsdokumenten sind.

Unter der Verantwortung des Generaldirektors nimmt es folgende Aufgaben wahr:

a) Verwaltung der Registrierung, Vervielfältigung, Übersetzung, Weiterleitung, Versendung und Vernichtung der Informationen;

b) Führung des Verschlusssachenregisters;

c) regelmäßige Anfragen bei den Urhebern, ob die Einstufung der betreffenden Informationen aufrechtzuerhalten ist;

d) im Benehmen mit dem ESA-Sicherheitsbüro Festlegung des praktischen Vorgehens bei der Einstufung und der Aufhebung des Geheimhaltungsgrades von Informationen.

41. Das Verschlusssachenbüro führt ein Register mit folgenden Angaben:

a) Datum der Erstellung der Verschlusssache,

b) Geheimhaltungsgrad,
c) Sperrfrist,
d) Name und Dienststelle des Urhebers,
e) der oder die Empfänger mit laufender Nummer,
f) Gegenstand,
g) Nummer,
h) Zahl der verbreiteten Exemplare,
i) Erstellung von Bestandsverzeichnissen der dem Rat unterbreiteten Verschlusssachen,
j) Register betreffend die Aufhebung des Geheimhaltungsgrades und die Herabstufung von Verschlusssachen.

42. Für das Verschlusssachenbüro der ESA-Hauptverwaltung gelten die allgemeinen Vorschriften der Kapitel I bis V dieses Abschnitts, soweit sie nicht durch die besonderen Vorschriften dieses Kapitels geändert werden.

ABSCHNITT VIII
ESA-ZENTRALREGISTRATUREN

„ESA STRENG GEHEIM“-REGISTRATUREN

1. Durch eine „ESA STRENG GEHEIM“-Zentralregistratur wird gewährleistet, dass die Registrierung, Handhabung und Verteilung von „ESA STRENG GEHEIM“-Dokumenten gemäß diesen Sicherheitsvorschriften erfolgt. Der Leiter der „ESA STRENG GEHEIM“-Registratur in der ESA bzw. in jedem Mitgliedstaat ist der „ESA STRENG GEHEIM“-Registraturkontrollbeauftragte.
2. Die „ESA STRENG GEHEIM“-Zentralregistratur ist die hauptsächliche Empfangs- und Versandbehörde in der ESA sowie gegebenenfalls in den Mitgliedstaaten, internationalen Organisationen und Drittstaaten, mit denen die ESA Abkommen über die Sicherheitsverfahren für den Austausch von Verschlusssachen geschlossen hat.
3. Nötigenfalls werden Unterregistraturen eingerichtet, die für die interne Verwaltung von „ESA STRENG GEHEIM“-Dokumenten zuständig sind; sie führen ein Register der von ihnen aufbewahrten Dokumente, das stets auf dem neuesten Stand gehalten wird.
4. „ESA STRENG GEHEIM“-Unterregistraturen werden nach Maßgabe des Abschnitts I Nummer 2 Buchstabe b eingerichtet, damit längerfristigen Notwendigkeiten entsprochen werden kann; sie werden einer „ESA STRENG GEHEIM“-Zentralregistratur zugeordnet. Müssen „ESA STRENG GEHEIM“-Dokumente nur zeitweilig und gelegentlich konsultiert werden, so können sie ohne Einrichtung einer „ESA STRENG GEHEIM“-Unterregistratur weitergeleitet werden, sofern Vorschriften festgelegt wurden, die gewährleisten, dass diese Dokumente unter der Kontrolle der entsprechenden „ESA STRENG GEHEIM“-Registratur verbleiben und alle materiellen und personenbezogenen Sicherheitsmaßnahmen eingehalten werden.
5. Unterregistraturen ist es nicht gestattet, ohne ausdrückliche Zustimmung ihrer „ESA STRENG GEHEIM“-Zentralregistratur „ESA STRENG GEHEIM“-Dokumente unmittelbar an andere Unterregistraturen derselben Zentralregistratur zu übermitteln.
6. Der Austausch von „ESA STRENG GEHEIM“-Dokumenten zwischen Unterregistraturen, die nicht derselben Zentralregistratur zugeordnet sind, muss über die „ESA STRENG GEHEIM“-Zentralregistraturen abgewickelt werden.

DIE „ESA STRENG GEHEIM“-ZENTRALREGISTRATUR

7. In seiner Eigenschaft als Kontrollbeauftragter ist der Leiter der „ESA STRENG GEHEIM“-Zentralregistratur zuständig für
   a) die Übermittlung von „ESA STRENG GEHEIM“-Dokumenten gemäß den in Abschnitt VII festgelegten Vorschriften;
   b) die Führung einer Liste aller ihm unterstehenden „ESA STRENG GEHEIM“-Unterregistraturen mit Name und Unterschrift der ernannten Kontrollbeauftragten und ihrer bevollmächtigten Stellvertreter;
   c) die Aufbewahrung der Empfangsbescheinigungen der Registraturen für alle von der Zentralregistratur verteilten „ESA STRENG GEHEIM“-Dokumente;
   d) die Führung eines Registers aller aufbewahrten und verteilten „ESA STRENG GEHEIM“-Dokumente;

e) die Führung einer aktuellen Liste aller „ESA STRENG GEHEIM“-Zentralregistraturen, mit denen er üblicherweise korrespondiert, mit Name und Unterschrift der ernannten Kontrollbeauftragten und ihrer bevollmächtigten Stellvertreter;

f) den materiellen Schutz aller in der Registratur aufbewahrten „ESA STRENG GEHEIM“-Dokumente gemäß den Vorschriften des Abschnitts IV.

„ESA STRENG GEHEIM“-UNTERREGISTRATUREN

8. In seiner Eigenschaft als Kontrollbeauftragter ist der Leiter einer „ESA STRENG GEHEIM“-Unterregistratur zuständig für

a) die Übermittlung von „ESA STRENG GEHEIM“-Dokumenten gemäß den in Abschnitt VII und Abschnitt VIII Nummern 5 und 6 festgelegten Vorschriften;

b) die Führung einer aktuellen Liste aller Personen, die befugt sind, Zugang zu den „ESA STRENG GEHEIM“-Informationen zu erhalten, welche seiner Aufsicht unterliegen;

c) die Verteilung von „ESA STRENG GEHEIM“-Dokumenten gemäß den Anweisungen des Urhebers oder nach dem Grundsatz „Kenntnis nur wenn nötig“, nach vorheriger Prüfung, ob der Empfänger die erforderliche Sicherheitsermächtigung besitzt;

d) die Führung eines auf neuestem Stand zu haltenden Registers aller aufbewahrten oder in Umlauf befindlichen „ESA STRENG GEHEIM“-Dokumente, die seiner Aufsicht unterliegen oder die an andere „ESA STRENG GEHEIM“-Registraturen weitergeleitet wurden, und Aufbewahrung aller entsprechenden Empfangsbescheinigungen;

e) die Führung einer aktuellen Liste der „ESA STRENG GEHEIM“-Registraturen, mit denen er „ESA STRENG GEHEIM“-Dokumente austauschen darf, mit Name und Unterschrift ihrer Kontrollbeauftragten und bevollmächtigten Stellvertreter;

f) den materiellen Schutz aller in der Unterregistratur aufbewahrten „ESA STRENG GEHEIM“-Dokumente gemäß den Vorschriften des Abschnitts IV.

BESTANDSAUFNAHMEN

9. Alle zwölf Monate führt jede „ESA STRENG GEHEIM“-Registratur eine ausführliche Bestandsaufnahme aller „ESA STRENG GEHEIM“-Dokumente durch, für die sie nachweispflichtig ist. Als nachgewiesen gilt jedes Dokument, das in der Registratur materiell vorhanden ist oder für das die Empfangsbescheinigung einer „ESA STRENG GEHEIM“-Registratur, der das Dokument übermittelt wurde, bzw. eine Vernichtungsbescheinigung oder aber eine Anweisung zur Herabstufung dieses Dokuments oder zur Aufhebung seines Geheimhaltungsgrades vorliegt.

10. Die „ESA STRENG GEHEIM“-Unterregistraturen übermitteln die Ergebnisse ihrer jährlichen Bestandsaufnahme der Zentralregistratur, der sie unterstehen, zu einem von dieser festgelegten Datum.

11. Die NSA/DSA sowie die ESA-Niederlassungen und internationalen Organisationen, in denen eine „ESA STRENG GEHEIM“-Zentralregistratur eingerichtet wurde, übermitteln dem Generaldirektor spätestens zum 1. April eines jeden Jahres die Ergebnisse der jährlichen Bestandsaufnahme ihrer „ESA STRENG GEHEIM“-Zentralregistraturen.

ABSCHNITT IX

SICHERHEITSMASSNAHMEN BEI BESONDEREN TAGUNGEN AUSSERHALB DER HAUPTVERWALTUNG, NIEDERLASSUNGEN UND ANLAGEN DER ESA, BEI DENEN HOCHEMPFINDLICHE ANGELEGENHEITEN ERÖRTERT WERDEN

ALLGEMEINES

1. Finden ESA-Ratstagungen auf Ministerebene oder andere wichtige Tagungen außerhalb der ESA-Hauptverwaltung in Paris oder außerhalb ihrer Niederlassungen und Anlagen statt und ist es durch die besonderen Sicherheitsanforderungen aufgrund der hohen Empfindlichkeit der behandelten Fragen oder Informationen gerechtfertigt, so werden die nachstehend beschriebenen Sicherheitsmaßnahmen ergriffen. Diese Maßnahmen betreffen lediglich den Schutz von ESA-Verschlusssachen; möglicherweise sind weitere Sicherheitsmaßnahmen vorzusehen.

VERANTWORTLICHKEITEN

Gastgebender Mitgliedstaat

2. Der Mitgliedstaat, in dessen Hoheitsgebiet eine ESA-Ratstagung auf Ministerebene oder eine andere wichtige Tagung stattfindet (gastgebender Mitgliedstaat), sollte in Zusammenarbeit mit dem ESA-Sicherheitsbüro für die Sicherheit dieser Tagung verantwortlich sein.

In bezug auf den Sicherheitsschutz sollte er insbesondere gewährleisten, dass

a) Pläne für den Umgang mit Sicherheitsrisiken und sicherheitsrelevanten Zwischenfällen aufgestellt werden, wobei die betreffenden Maßnahmen insbesondere auf die sichere Verwahrung von ESA-Verschlusssachen in Büroräumen abzielen;

b) Maßnahmen getroffen werden, um gegebenenfalls Zugang zum Kommunikationssystem des ESA-Rates für den Empfang und die Versendung von als Verschlusssache eingestuften ESA-Nachrichten zu gewähren. Ferner wird der gastgebende Mitgliedstaat erforderlichenfalls Zugang zu sicheren Telefonsystemen gewähren.

Mitgliedstaaten

3. Die Behörden der Mitgliedstaaten sollten die erforderlichen Maßnahmen treffen, um dafür zu sorgen, dass

a) für ihre nationalen Delegierten geeignete Sicherheitsunbedenklichkeitsbescheinigungen bereitgestellt und erforderlichenfalls per Signalübertragung oder Fax entweder unmittelbar oder über das ESA-Sicherheitsbüro dem Sicherheitsbeauftragten für die betreffende Tagung übermittelt werden;

b) alle besonderen Risiken den Behörden des gastgebenden Mitgliedstaats und erforderlichenfalls dem ESA-Sicherheitsbüro mitgeteilt werden, so dass geeignete Abhilfemaßnahmen getroffen werden können.

Sicherheitsbeauftragter für die Tagung

4. Es wird ein Sicherheitsbeauftragter ernannt, der für die allgemeine Vorbereitung und Überwachung der allgemeinen internen Sicherheitsmaßnahmen und für die Koordinierung mit den anderen betroffenen Sicherheitsbehörden verantwortlich ist.

ESA-Sicherheitsbüro

5. Das ESA-Sicherheitsbüro sollte als Sicherheitsberatungsstelle für die Vorbereitung der Tagung fungieren; es sollte auf der Tagung vertreten sein, um erforderlichenfalls den Sicherheitsbeauftragten für die Tagung und die Delegationen zu unterstützen und zu beraten.

SICHERHEITSMASSNAHMEN

Sicherheitsbereiche

6. Es werden folgende Sicherheitsbereiche angelegt:

a) ein Sicherheitsbereich der Kategorie II, der nach Maßgabe der Erfordernisse einen Redaktionsraum, die Büroräume der ESA und die Vervielfältigungsausrüstung sowie die Büroräume der Delegationen umfasst;

b) ein Sicherheitsbereich der Kategorie I, der den Konferenzraum sowie die Dolmetschkabinen und die Kabinen für die Tontechnik umfasst;

c) Verwaltungsbereiche, die aus dem Pressebereich und den für Verwaltung, Verpflegung und Unterkunft genutzten Bereichen des Tagungsortes sowie aus dem sich unmittelbar an das Pressezentrum und den Tagungsort anschließenden Bereich bestehen.

Berechtigungsausweise

7. Der Sicherheitsbeauftragte für die Tagung sollte entsprechend dem von den Delegationen gemeldeten Bedarf geeignete Berechtigungsausweise ausgeben. Erforderlichenfalls kann eine Abstufung der Zugangsberechtigung für die verschiedenen Sicherheitsbereiche vorgesehen werden.

Kontrolle von fotografischen Ausrüstungen und Tonaufzeichnungsgeräten

8. Bild- oder Tonaufzeichnungsgeräte, mit Ausnahme der Geräte für die offizielle Aufzeichnung, und Mobilfunktelefone dürfen nicht in einen Sicherheitsbereich der Kategorie I gebracht werden, sofern es sich nicht um die Ausrüstung von Fotografen und Tontechnikern handelt, die vom Sicherheitsbeauftragten für die Tagung vorschriftsgemäß zugelassen worden sind.

Überprüfung der Büroräume

9. Der Sicherheitsbeauftragte für die Tagung hat dafür zu sorgen, dass die Büroräume der ESA-Exekutive und der Delegationen am Ende jedes Arbeitstages überprüft werden, damit sichergestellt ist, dass alle ESA-Verschlusssachen an einem sicheren Ort aufbewahrt werden; andernfalls hat er die erforderlichen Abhilfemaßnahmen zu treffen.

Abfallbeseitigung bei ESA-Verschlusssachen

10. Sämtliche Abfälle sind als ESA-Verschlusssachen zu behandeln, und die ESA-Exekutive und die Delegationen erhalten zur Entsorgung Papierkörbe oder Abfallsäcke. Die ESA-Exekutive und die

Delegationen bringen vor Verlassen der ihnen zugewiesenen Räumlichkeiten die Abfälle zum Sicherheitsbeauftragten für die Tagung, der ihre Vernichtung nach diesen Vorschriften veranlasst.

ABSCHNITT X
VERLETZUNG DER SICHERHEIT UND KENNTNISNAHME VON ESA-VERSCHLUSSSACHEN DURCH UNBEFUGTE

1. Zu einer Verletzung der Sicherheit kommt es, wenn durch eine Handlung oder durch eine Unterlassung, die den ESA- oder nationalen Sicherheitsvorschriften zuwiderläuft, ESA-Verschlusssachen in Gefahr geraten oder Unbefugten zur Kenntnis gelangen könnten.
2. Eine Kenntnisnahme von ESA-Verschlusssachen durch Unbefugte liegt vor, wenn die Verschlusssachen ganz oder teilweise in die Hände unbefugter Personen (d. h. von Personen, die nicht die erforderliche Zugangsermächtigung haben oder deren Kenntnis der Verschlusssachen nicht nötig ist) gelangt sind oder es wahrscheinlich ist, dass eine derartige Kenntnisnahme stattgefunden hat.
3. Die Kenntnisnahme von ESA-Verschlusssachen durch Unbefugte kann die Folge von Nachlässigkeit, Fahrlässigkeit oder Indiskretion, aber auch der Tätigkeit von Diensten, die in der ESA oder ihren Mitgliedstaaten Kenntnis von ESA-Verschlusssachen und geheimen Tätigkeiten erlangen wollen, oder von subversiven Organisationen sein.
4. Es ist wichtig, dass alle Personen, die mit ESA-Verschlusssachen umgehen müssen, eingehend über die Sicherheitsverfahren, die Gefahren von indiskreten Gesprächen und über ihre Beziehungen zur Presse unterrichtet werden. Sie sollten sich darüber im klaren sein, wie wichtig es ist, jede ihnen bekannt werdende Verletzung der Sicherheit sofort der zuständigen Sicherheitsbehörde des Mitgliedstaats bzw. dem Sicherheitsbeauftragten der ESA-Hauptverwaltung, -Niederlassung oder -Anlage, in dem bzw. der sie beschäftigt sind, mitzuteilen.
5. Wenn eine Sicherheitsbehörde eine Verletzung der Sicherheit betreffend ESA-Verschlusssachen oder den Verlust bzw. das Verschwinden von als ESA-Verschlusssache eingestuftem Material entdeckt oder hiervon unterrichtet wird, trifft sie rasch Maßnahmen, um
   a) Beweise zu sichern;
   b) den Sachverhalt zu klären;
   c) den entstandenen Schaden zu bewerten und möglichst klein zu halten;
   d) zu verhindern, dass sich ein derartiger Vorfall wiederholt;
   e) die zuständigen Behörden von den Folgen der Verletzung der Sicherheit zu unterrichten.

   In diesem Zusammenhang sind folgende Angaben zu machen:
      i) eine Beschreibung der entsprechenden Verschlusssache unter Angabe ihres Geheimhaltungsgrades, ihres Aktenzeichens und der Ausfertigungsnummer, des Datums, des Urhebers, des Themas und des Umfangs;
      ii) eine kurze Beschreibung der Umstände, unter denen die Verletzung der Sicherheit erfolgt ist, unter Angabe des Datums und des Zeitraums, während dessen die Verschlusssache Unbefugten zur Kenntnis gelangen konnte;
      iii) eine Erklärung darüber, ob der Urheber informiert worden ist.
6. Jede Sicherheitsbehörde hat die Pflicht, unmittelbar nach ihrer Unterrichtung von einer möglichen Verletzung der Sicherheit dem ESA-Sicherheitsbüro hierüber Bericht zu erstatten. Ist die Kenntnisnahme von ESA-Verschlusssachen durch Unbefugte im Zuständigkeitsbereich eines Mitgliedstaates erfolgt, so wird sie über die zuständige NSA/DSA auf die in Nummer 5 angegebene Weise dem ESA-Sicherheitsbüro gemeldet.
7. Fälle, in denen es um als „ESA NUR FÜR DEN DIENSTGEBRAUCH“ eingestufte Verschlusssachen geht, müssen nur dann gemeldet werden, wenn sie ungewöhnlicher Art sind.
8. Wird der Generaldirektor von einer Verletzung der Sicherheit unterrichtet, so
   a) unterrichtet er die Stelle, von der die entsprechende Verschlusssache stammt;
   b) bittet er die zuständigen Sicherheitsbehörden um die Einleitung von Ermittlungen;
   c) koordiniert er die Ermittlungen, falls mehr als eine Sicherheitsbehörde betroffen ist;
   d) lässt er einen Bericht erstellen über die Umstände der Verletzung der Sicherheit, das Datum oder den Zeitraum, an dem bzw. während dessen die Verletzung erfolgt ist und der Verstoß entdeckt wurde; der Bericht umfasst eine detaillierte Beschreibung des Inhalts und des Geheimhaltungsgrades des betreffenden Materials. Es sollte auch berichtet werden, welcher

Schaden den Interessen der ESA oder eines oder mehrerer ihrer Mitgliedstaaten entstanden ist und welche Maßnahmen ergriffen worden sind, um eine Wiederholung des Vorfalls zu verhindern.

9. Die Stelle, von der die Verschlusssache stammt, unterrichtet deren Empfänger und gibt ihnen entsprechende Anweisungen.
10. Gegen jede für die Kenntnisnahme von ESA-Verschlusssachen durch Unbefugte verantwortliche Person können disziplinarische Maßnahmen auf Grund der geltenden Vorschriften und Regelungen ergriffen werden. Diese Maßnahmen lassen etwaige andere rechtliche Verfahren unberührt. Die ESA-Bediensteten und -Sachverständigen sind von den möglichen rechtlichen Folgen von Verletzungen der Sicherheit und vor allem von der in Artikel 7 des Sicherheitsübereinkommens vorgesehenen Möglichkeit der Aufhebung ihrer Immunität in Kenntnis zu setzen.

ABSCHNITT XI

SCHUTZ VON ESA-VERSCHLUSSSACHEN IN INFORMATIONSTECHNISCHEN SYSTEMEN UND KOMMUNIKATIONSSYSTEMEN

Kapitel I

Einleitung

ALLGEMEINES

1. Das Sicherheitskonzept und die Sicherheitsanforderungen, die in diesem Abschnitt beschrieben werden, gelten für alle Kommunikations- und Informationssysteme und -netze (nachstehend als SYSTEME bezeichnet), in denen ESA-Verschlusssachen verarbeitet werden.
2. Bei allen SYSTEMEN sind Sicherheitsmaßnahmen zum Schutz der Integrität und der Verfügbarkeit dieser SYSTEME und der darin enthaltenen Informationen erforderlich. Bei SYSTEMEN, die ESA-Verschlusssachen enthalten, sind zudem Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit dieser Informationen erforderlich. Die auf diese SYSTEME anzuwendenden Sicherheitsmaßnahmen werden von der dazu vorgesehenen Akkreditierungsstelle für IT-Sicherheit (Security Accreditation Authority, SAA) festgelegt; sie entsprechen dem festgestellten Risiko und stehen mit dem in diesen Sicherheitsvorschriften dargelegten Konzept im Einklang.
   Das IT-Sicherheitskonzept der ESA stützt sich auf folgende Grundsätze:
   - Es ist Bestandteil der Sicherheit im allgemeinen und ergänzt alle Teilaspekte der Datensicherheit, der Sicherheit des Personals und der materiellen Sicherheit;
   - Aufteilung der Zuständigkeiten auf Eigentümer der technischen SYSTEME, Eigentümer von ESA-Verschlusssachen, die in technischen SYSTEMEN gespeichert oder verarbeitet werden, IT-Sicherheitsexperten und Nutzer;
   - Beschreibung der Sicherheitsgrundsätze und Anforderungen jedes IT-SYSTEMS;
   - Genehmigung dieser Grundsätze und Anforderungen durch die vorgesehene Akkreditierungsstelle für IT-Sicherheit (SAA);
   - Berücksichtigung der spezifischen Bedrohungen und Schwachstellen in der IT-Umgebung.
3. Der Schutz eingebetteter IT-SYSTEME wird im allgemeinen Kontext der SYSTEME, deren Bestandteil sie sind, unter weitestgehender Anwendung der jeweiligen Bestimmungen dieses Abschnitts festgelegt und spezifiziert.

BEDROHUNGEN UND SCHWACHSTELLEN VON SYSTEMEN

4. Eine Bedrohung kann allgemein als Möglichkeit einer unabsichtlichen oder absichtlichen Beeinträchtigung der Sicherheit definiert werden. Bei SYSTEMEN ist dies mit dem Verlust einer oder mehrerer der Eigenschaften Vertraulichkeit, Integrität und Verfügbarkeit verbunden. Eine Schwachstelle kann als unzureichende oder fehlende Kontrolle definiert werden, die die Bedrohung eines bestimmten Objekts oder Ziels erleichtern oder ermöglichen könnte. Eine Schwachstelle kann durch ein Versäumnis entstehen, oder sie kann mit nachlässigen, unvollständigen oder inkonsistenten Kontrollen zusammenhängen; sie kann die Technik, die Verfahrens- oder die Betriebsebene betreffen.
5. ESA-Verschlusssachen und sonstige Informationen, die in SYSTEMEN in einer zur raschen Abfrage, Übermittlung und Nutzung konzipierten konzentrierten Form vorliegen, sind in vielerlei Hinsicht (durch eine Kombinationen von Bedrohungen und Schwachstellen) gefährdet. So könnten z. B. Unbefugte auf die Informationen zugreifen, oder Befugten könnte der Zugriff verweigert werden. Ferner besteht das Risiko einer unerlaubten Verbreitung, einer Verfälschung, Ände-

rung oder Löschung der Informationen. Außerdem sind die komplexen und manchmal empfindlichen Geräte teuer in der Anschaffung, und es ist häufig schwierig, sie rasch zu reparieren oder zu ersetzen. Deshalb stellen diese SYSTEME attraktive Ziele für geheimdienstliche Tätigkeit oder Sabotage dar, insbesondere wenn die Sicherheitsmaßnahmen für unzureichend gehalten werden.

SICHERHEITSMASSNAHMEN

6. Die in diesem Abschnitt festgelegten Sicherheitsmaßnahmen dienen in erster Linie dem Schutz von Informationen vor unerlaubter Preisgabe (Verlust der Vertraulichkeit) sowie dem Schutz vor dem Verlust der Integrität oder der Verfügbarkeit von Informationen. Um ein SYSTEM, in dem ESA-Verschlusssachen verarbeitet werden, angemessen zu schützen, sind gemäß dem Geheimhaltungsgrad der zu schützenden ESA-Verschlusssache die einschlägigen konventionellen Sicherheitsnormen anzuwenden, zu denen geeignete, auf das jeweilige SYSTEM zugeschnittene spezielle Sicherheitsverfahren und -techniken hinzukommen.
7. Um ein sicheres Umfeld für den Betrieb eines SYSTEMS zu schaffen, muss eine ausgewogene Kombination von Sicherheitsmaßnahmen ausgewählt und umgesetzt werden. Diese Maßnahmen betreffen physische Objekte, das Personal, nichttechnische Verfahren sowie Betriebsverfahren für Computer und Kommunikationssysteme.
8. Bei Maßnahmen im Bereich der Computersicherheit (Sicherheitseigenschaften der Hard- und Software) muss der Grundsatz des berechtigen Informationsbedarfs (Prinzip „Kenntnis nur wenn nötig“) eingehalten werden, und die unerlaubte Preisgabe von Informationen muss verhindert oder aufgedeckt werden. Wie zuverlässig Maßnahmen der Computersicherheit sein müssen, wird bei der Formulierung der Sicherheitsanforderungen festgelegt. Im Rahmen der Akkreditierung wird überprüft, dass eine angemessene Vertrauenswürdigkeit vorhanden ist, um sich auf Maßnahmen der Computersicherheit verlassen zu können.

AUFSTELLUNG DER SYSTEMSPEZIFISCHEN SICHERHEITSANFORDERUNGEN (SSRS)

9. Für alle SYSTEME, in denen als „ESA VERTRAULICH“ oder höher eingestufte Informationen verarbeitet werden, ist eine Aufstellung der systemspezifischen Sicherheitsanforderungen (SSRS) erforderlich, die von der für den Betrieb des IT-SYSTEMS zuständigen Stelle (ITSOA) bzw. dem Eigentümer des technischen SYSTEMS (TSO) und dem Eigentümer der Informationen, gegebenenfalls mit Beiträgen und Unterstützung des Projektpersonals und der INFOSEC-Stelle, erstellt und von der Akkreditierungsstelle für IT-Sicherheit (SAA) genehmigt wird. Eine SSRS ist auch dann erforderlich, wenn die Vertraulichkeit, Verfügbarkeit und Integrität von als „ESA NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Informationen oder von Informationen ohne VS-Einstufung von der SAA als sicherheitskritisch angesehen wird.
10. Die SSRS wird im frühesten Stadium der Konzeption eines Projekts formuliert und parallel zum Projektverlauf weiterentwickelt und verbessert; sie erfüllt unterschiedliche Aufgaben in verschiedenen Stadien des Projekts und des Lebenszyklus des SYSTEMS.
11. Die SSRS wird zwischen der für den Betrieb des IT-Systems zuständigen Stelle bzw. dem Eigentümer des technischen SYSTEMS (TSO) und dem Eigentümer der Informationen und der SAA verbindlich vereinbart und bei der Akkreditierung des SYSTEMS zugrunde gelegt.
12. Die SSRS ist eine vollständige und ausführliche Festlegung der einzuhaltenden Sicherheitsgrundsätze und der zu erfüllenden detaillierten Sicherheitsanforderungen. Sie beruht auf den Sicherheitsvorschriften und der Risikobewertung der ESA bzw. wird von Faktoren des betrieblichen Umfelds bestimmt, vom jeweiligen Sicherheitsmodus oder den Benutzeranforderungen. Die SSRS ist Bestandteil der Projektdokumentation, die den zuständigen Stellen zur Billigung der technischen, haushaltsbezogenen und sicherheitsrelevanten Aspekte unterbreitet wird. In ihrer endgültigen Fassung ist die SSRS eine vollständige Beschreibung der Voraussetzungen, die gegeben sein müssen, damit ein bestimmtes SYSTEM sicher ist.

SICHERHEITSMODUS

13. Alle SYSTEME, in denen als „ESA VERTRAULICH“ oder höher eingestufte Informationen verarbeitet werden, werden für den Betrieb in einem einzigen Sicherheitsmodus oder – aufgrund zeitlich unterschiedlicher Anforderungen – in mehreren der folgenden sicherheitsbezogenen Betriebsarten (oder deren einzelstaatlichen Entsprechungen) freigegeben:

    a) „dedicated“;

    b) „system high“;

    c) „multi-level“.

Kapitel II

ZUSÄTZLICHE KENNZEICHNUNGEN

14. Zusätzliche Kennzeichnungen wie z. B. CRYPTO oder eine andere von der ESA anerkannte Sonderkennung werden verwendet, wenn zusätzlich zu der Behandlung, die sich durch die VS-Einstufung ergibt, eine begrenzte Verteilung und eine besondere Abwicklung erforderlich sind.

BEGRIFFSBESTIMMUNGEN

15. Der SICHERHEITSMODUS „DEDICATED“ bezeichnet eine Betriebsart, bei der ALLE Personen, die Zugang zum SYSTEM haben, zum Zugriff auf den höchsten im SYSTEM verarbeiteten Geheimhaltungsgrad berechtigt sind und generell einen berechtigten Informationsbedarf in bezug auf ALLE im SYSTEM verarbeiteten Informationen haben.

Anmerkungen:

(1) Da alle Nutzer einen berechtigten Informationsbedarf haben, muss sicherheitstechnisch nicht unbedingt zwischen unterschiedlichen Informationen innerhalb des SYSTEMS unterschieden werden.

(2) Andere Sicherheitseigenschaften (z. B. objekt-, personen- und verfahrensbezogene Funktionen) müssen den Anforderungen für den höchsten Geheimhaltungsgrad und für alle Kategorien von Informationen, die im SYSTEM verarbeitet werden, entsprechen.

16. Der SICHERHEITSMODUS „SYSTEM HIGH“ bezeichnet eine Betriebsart, bei der ALLE Personen, die Zugang zum SYSTEM haben, zum Zugriff auf den höchsten im SYSTEM verarbeiteten Geheimhaltungsgrad berechtigt sind, bei der aber NICHT ALLE Personen, die Zugang zum SYSTEM haben, generell einen berechtigten Informationsbedarf in bezug auf die im SYSTEM verarbeiteten Informationen haben.

Anmerkungen:

(1) Da nicht alle Nutzer generell einen berechtigten Informationsbedarf haben, muss die sicherheitstechnische Ausgestaltung einen selektiven Zugriff auf Informationen und eine Trennung von Informationen innerhalb des SYSTEMS gewährleisten.

(2) Andere Sicherheitseigenschaften (z. B. objekt-, personen- und verfahrensbezogene Funktionen) müssen den Anforderungen für den höchsten Geheimhaltungsgrad und für alle Kategorien von Informationen, die im SYSTEM verarbeitet werden, entsprechen.

(3) Bei dieser Betriebsart werden alle im SYSTEM verarbeiteten oder für das SYSTEM verfügbaren Informationen sowie die entsprechenden Ausgaben – solange nichts anderes festgelegt wurde – so geschützt, als würden sie unter die jeweilige Kategorie von Informationen und den höchsten verarbeiteten Geheimhaltungsgrad fallen, es sei denn, eine vorhandene Kennzeichnungsfunktion ist in ausreichendem Maße vertrauenswürdig.

17. Der SICHERHEITSMODUS „MULTI-LEVEL“ bezeichnet eine Betriebsart, bei der NICHT ALLE Personen, die Zugang zum SYSTEM haben, zum Zugriff auf den höchsten Geheimhaltungsgrad im SYSTEM berechtigt sind und bei der NICHT ALLE Personen, die Zugang zum SYSTEM haben, generell einen berechtigten Informationsbedarf in bezug auf die im SYSTEM verarbeiteten Informationen haben.

Anmerkungen:

(1) In dieser Betriebsart ist derzeit die Verarbeitung von Informationen unterschiedlicher Geheimhaltungsgrade und verschiedener Kategorien von Informationen möglich.

(2) Da nicht alle Personen zum Zugriff auf die höchsten Geheimhaltungsgrade berechtigt sind, und da nicht alle Personen generell einen berechtigten Informationsbedarf in bezug auf die im SYSTEM verarbeiteten Informationen haben, muss die sicherheitstechnische Ausgestaltung einen selektiven Zugriff auf Informationen und eine Trennung von Informationen innerhalb des SYSTEMS gewährleisten.

18. INFORMATIONSSICHERHEIT (INFOSEC) bezeichnet die Anwendung von Sicherheitsmaßnahmen zum Schutz von Informationen, die in Kommunikations- und Informationssystemen und anderen elektronischen Systemen verarbeitet, gespeichert oder übermittelt werden, vor dem unabsichtlichen oder absichtlichen Verlust der Vertraulichkeit, Integrität und Verfügbarkeit, sowie zur Vermeidung des Verlustes der Integrität und Verfügbarkeit der SYSTEME selbst. INFOSEC-Maßnahmen erstrecken sich auf die Sicherheit von Computern, die Sicherheit der Übertragung, die Sicherheit vor Abstrahlung und die kryptographische Sicherheit sowie die Aufdeckung, Dokumentation und Bekämpfung von Bedrohungen für Informationen und SYSTEME.

19. COMPUTERSICHERHEIT (COMPUSEC) bezeichnet den Einsatz der Sicherheitseigenschaften von Hardware, Firmware und Software eines Computersystems zum Schutz vor unerlaubter Preisgabe, Manipulation, Änderung bzw. Löschung von Informationen sowie vor einem Systemausfall (Denial of Service).
20. COMPUTERSICHERHEITSPRODUKT ist ein allgemeines, der Computersicherheit dienendes Produkt, das zur Integration in ein IT-SYSTEM und zur Verbesserung bzw. Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen bestimmt ist.
21. KOMMUNIKATIONSSICHERHEIT (COMSEC) bezeichnet die Anwendung von Sicherheitsmaßnahmen auf den Telekommunikationsverkehr, um zu verhindern, dass Unbefugte in den Besitz wertvoller Informationen gelangen, die aus dem Zugriff auf den Telekommunikationsverkehr und dessen Auswertung gewonnen werden könnten, oder um die Vertraulichkeit und Integrität des Telekommunikationsverkehrs sicherzustellen.

Anmerkung:

Diese Maßnahmen umfassen die kryptographische Sicherheit, die Sicherheit der Übermittlung und die Sicherheit vor Abstrahlung und ferner die verfahrens-, objekt- und personenbezogene Sicherheit sowie die Dokumenten- und Computersicherheit.

22. PRODUKT FÜR KRYPTOGRAPHISCHE SICHERHEIT ist ein allgemeines, der Kommunikationssicherheit dienendes Produkt, das zur Integration in ein Kommunikationssystem und zur Verbesserung bzw. Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen bestimmt ist.
23. EVALUATION bezeichnet die eingehende technische Prüfung der Sicherheitsaspekte eines SYSTEMS oder eines Produkts für kryptographische Sicherheit oder Computersicherheit durch eine zuständige Stelle.

Anmerkungen:

(1) Bei der Evaluation wird geprüft, ob die verlangten Sicherheitsfunktionen tatsächlich vorhanden sind und ob sie negative Nebeneffekte haben, und es wird bewertet, inwieweit diese Funktionen verfälscht werden könnten.

(2) Bei der Evaluation wird ferner bestimmt, inwieweit die für ein SYSTEM geltenden Sicherheitsanforderungen erfüllt bzw. die geltend gemachten Sicherheitsleistungen eines Computersicherheitsprodukts erbracht werden, und es wird die Vertrauenswürdigkeitsstufe des SYSTEMS oder des Produkts für kryptographische Sicherheit oder Computersicherheit bestimmt.

24. ZERTIFIZIERUNG bezeichnet eine – durch eine unabhängige Überprüfung der Durchführung und der Ergebnisse einer Evaluation gestützte – förmliche Bescheinigung der zuständigen Akkreditierungsstelle darüber, inwieweit ein SYSTEM die Sicherheitsanforderungen erfüllt oder inwieweit ein Produkt für kryptographische Sicherheit oder Computersicherheit vorgegebene Sicherheitsleistungen erbringt.
25. GENEHMIGUNG ZUR VERWENDUNG eines Produkts für kryptographische Sicherheit bezeichnet eine – durch die Ergebnisse einer Evaluation gestützte – förmliche Bescheinigung einer Nationalen Zulassungsstelle mit eigenen Zulassungskriterien. Es handelt sich dabei um eine notwendige, aber nicht ausreichende Voraussetzung für die Akkreditierung.
26. AKKREDITIERUNG bezeichnet die Zulassung eines SYSTEMS zur Verarbeitung von ESA-Verschluss-Sachen in seinem betrieblichen Umfeld.

Anmerkung:

Die Akkreditierung sollte erfolgen, nachdem alle einschlägigen sicherheitsrelevanten Verfahren durchgeführt worden sind und der Schutz der Systemressourcen in ausreichendem Maße sichergestellt worden ist. Die Akkreditierung sollte in der Regel auf der Grundlage der SSRS erfolgen und folgendes umfassen:

a) Festlegung der Zielvorgaben der Akkreditierung dieses SYSTEMS, insbesondere welche Geheimhaltungsgrade verarbeitet werden sollen und welcher Sicherheitsmodus für das SYSTEM oder Netz vorgeschlagen wird;

b) Bestandsaufnahme des Risikomanagements, in der Bedrohungen und Schwachstellen benannt und entsprechende Gegenmaßnahmen dargelegt werden;

c) sicherheitsbezogene Betriebsverfahren (SecOPs) mit einer detaillierten Beschreibung der vorgesehenen Abläufe (z. B. Betriebsarten und Funktionen) und mit einer Beschreibung der Sicherheitseigenschaften des SYSTEMS, die die Grundlage für die Akkreditierung bildet;

d) Plan für die Implementierung und Aufrechterhaltung der Sicherheitseigenschaften;

e) Plan für die erstmalige und nachfolgende Prüfung, Evaluation und Zertifizierung der SYSTEM- oder Netzsicherheit;

f) gegebenenfalls Zertifizierung zusammen mit anderen Teilaspekten der Akkreditierung.

g) Bei Produkten für kryptographische Sicherheit kann je nach Umfang der Änderungen gegenüber der genehmigten Fassung der SSRS eine Nachevaluation erforderlich sein.

27. IT-SYSTEM bezeichnet eine Gesamtheit von Betriebsmitteln, Methoden und Verfahren sowie gegebenenfalls Personal, die zusammenwirken, um Aufgaben der Informationsverarbeitung zu erfüllen.

Anmerkungen:

(1) Darunter wird eine Gesamtheit von Einrichtungen verstanden, die zur Verarbeitung von Informationen innerhalb des SYSTEMS konfiguriert sind.

(2) Diese SYSTEME können der Abfrage, der Steuerung, der Kontrolle, der Kommunikation und wissenschaftlichen oder administrativen Anwendungen einschließlich der Textverarbeitung dienen.

(3) Die Grenzen eines SYSTEMS werden im allgemeinen in bezug auf die Bestandteile definiert, die der Kontrolle einer einzigen ITSOA bzw. eines einzigen TSO unterliegen.

(4) Ein IT-SYSTEM kann Teilsysteme enthalten, von denen einige selbst wiederum IT-SYSTEME sind.

28. Die SICHERHEITSEIGENSCHAFTEN EINES IT-SYSTEMS umfassen alle Funktionen, Merkmale und Eigenschaften der Hardware, Firmware und Software; dazu gehören die Betriebsverfahren, die Nachvollziehbarkeit, die Zugangs- und Zugriffskontrollen, die IT-Umgebung, die Umgebung dezentraler Terminals bzw. Datenstationen, der vorgegebene Managementrahmen, die physischen Strukturen und Geräte sowie Personal- und Kommunikationskontrollen, die erforderlich sind, um einen annehmbaren Schutz der Verschlusssachen sicherzustellen, die in einem IT-SYSTEM verarbeitet werden sollen.

29. IT-NETZ bezeichnet eine Gesamtheit von geographisch verteilten IT-SYSTEMEN, die für den Datenaustausch miteinander verbunden sind; darin eingeschlossen sind die Bestandteile der vernetzten IT-SYSTEME sowie deren Schnittstelle mit den zugrundeliegenden Daten- oder Kommunikationsnetzen.

Anmerkungen:

(1) Ein IT-Netz kann die Funktionen eines oder mehrerer Kommunikationsnetze zum Datenaustausch nutzen; mehrere IT-Netze können die Funktionen eines gemeinsamen Kommunikationsnetzes nutzen.

(2) Ein IT-Netz wird als „lokal“ bezeichnet, wenn es mehrere am selben Standort befindliche Computer miteinander verbindet.

30. Die SICHERHEITSEIGENSCHAFTEN EINES IT-NETZES umfassen die Sicherheitseigenschaften der einzelnen IT-SYSTEME, aus denen das Netz besteht, sowie jene zusätzlichen Bestandteile und Eigenschaften, die mit dem Netz als solchem verbunden sind (z. B. Kommunikation im Netz, Mechanismen und Verfahren zur Sicherheitsidentifikation und zur Kennzeichnung, Zugriffskontrollen, Programme und automatische Ereignisprotokolle) und die erforderlich sind, um einen angemessenen Schutz der Verschlusssachen sicherzustellen.

31. IT-UMGEBUNG bezeichnet einen Bereich, in dem sich ein oder mehrere Computer, deren lokale Peripheriegeräte und Speichereinheiten, Steuereinheiten sowie ihnen fest zugeordnete Netz- und Kommunikationseinrichtungen befinden.

Anmerkung:

Nicht eingeschlossen sind davon abgetrennte Bereiche, in denen sich dezentrale Peripheriegeräte oder Terminals bzw. Datenstationen befinden, auch wenn diese an Geräte innerhalb der IT-Umgebung angeschlossen sind.

32. UMGEBUNG VON DEZENTRALEN TERMINALS bzw. DATENSTATIONEN bezeichnet einen Bereich außerhalb einer IT-Umgebung, in dem sich Computer, deren lokale Peripheriegeräte oder Terminals bzw. Datenstationen und alle zugehörigen Kommunikationseinrichtungen befinden.

33. TEMPEST-Schutzmaßnahmen (Transient Electromagnetic Pulse Emanation Standard) bezeichnen Sicherheitsmaßnahmen zum Schutz von Geräten und Kommunikationsinfrastruktur gegen die Preisgabe von Verschlusssachen durch unabsichtliche elektromagnetische Abstrahlung.

34. EIGENTÜMER DES TECHNISCHEN SYSTEMS (TSO) ist die für Einrichtung, Wartung, Betrieb und Abschaltung eines SYSTEMS zuständige Stelle.

Kapitel III

Zuständigkeiten im Sicherheitsbereich

ALLGEMEINES

35. Der Sicherheitsausschuss gemäß Abschnitt I Nummern 3 und 4 ist auch für INFOSEC-Fragen zuständig. Der Sicherheitsausschuss organisiert seine Tätigkeit so, dass er zu den vorstehenden Punkten sachverständigen Rat geben kann.
36. Das Sicherheitsbüro der ESA hat ein INFOSEC-Referat, das unter anderem dafür zuständig ist, auf der Grundlage dieses Kapitels ausführliche INFOSEC-Leitlinien aufzustellen.
37. Im Falle von Sicherheitsproblemen (Zwischenfälle, Verletzungen der Sicherheit usw.) wird die zuständige einzelstaatliche Behörde und/oder das Sicherheitsbüro der ESA sofort tätig. Alle Probleme werden dem Sicherheitsbüro der ESA gemeldet, das dafür verantwortlich ist, die Daten aufzuzeichnen und zu analysieren und gemäß Abschnitt X geeignete Maßnahmen zu ergreifen. Bei Verletzung oder Gefährdung der kryptographischen Sicherheit sind die Bestimmungen aus Kaptitel V dieses Abschnitts über Kommunikationssicherheit anzuwenden.

AKKREDITIERUNGSSTELLE FÜR IT-SICHERHEIT (SAA)

38. Die SAA ist entweder:
    - eine NSA oder andere zuständige Behörde, wenn das SYSTEM, in dem ESA-Verschlusssachen verarbeitet werden, unter nationaler Verantwortung steht,
    - der Leiter des Sicherheitsbüros der ESA, wenn das SYSTEM nicht mit einem nationalen Informationssystem verbunden ist und nicht nationale Verschlusssachen verwendet oder verarbeitet, oder
    - ein Gremium aus Vertretern der ESA und der zuständigen NSAs, wenn unterschiedliche Bestandteile des SYSTEMS in die Zuständigkeit der ESA und der Mitgliedstaaten fallen.
39. Die SAA hat sicherzustellen, dass die SYSTEME den Sicherheitsvorschriften der ESA entsprechen. Sie hat unter anderem die Aufgabe, ein SYSTEM zur Verarbeitung von ESA-Verschlusssachen bis zu einem bestimmten Geheimhaltungsgrad in seinem betrieblichen Umfeld zuzulassen.
    - Die Zuständigkeit der SAA der ESA erstreckt sich auf alle SYSTEME, die innerhalb der Räumlichkeiten der ESA (d.h. in der Hauptverwaltung, den Niederlassungen und den Anlagen der ESA) betrieben werden.
    - SYSTEME und Bestandteile von SYSTEMEN, die in einem Mitgliedstaat betrieben werden, verbleiben in der Zuständigkeit dieses Mitgliedstaats.
    - Wenn unterschiedliche Bestandteile eines SYSTEMS in die Zuständigkeit der SAA der ESA und anderer SAAs fallen, ernennen alle Parteien ein gemeinsames Akkreditierungsgremium, dessen Koordinierung die SAA der ESA unter Beteiligung von Vertretern der zuständigen NSA/DSA übernimmt.

INFOSEC-STELLE (IA)

40. Der Leiter des INFOSEC-Referats des ESA-Sicherheitsbüros ist die INFOSEC-Stelle für die ESA. Die INFOSEC-Stelle der ESA ist für folgendes verantwortlich:
    - Implementierung und Anwendung von Sicherheitseigenschaften eines SYSTEMS,
    - Überprüfung und Kontrolle der ordnungsgemäßen Anwendung der Sicherheitsvorschriften in der ESA,
    - technische Beratung und Unterstützung der SAA,
    - Unterstützung bei der Entwicklung der SSRS,
    - Überprüfung der SSRS auf ihre Übereinstimmung mit diesen Sicherheitsvorschriften und den Dokumenten über INFOSEC-Konzept und -Architektur,
    - Aufstellung ausführlicher INFOSEC-Leitlinien auf der Grundlage dieses Kapitels,
    - soweit erforderlich Teilnahme an den Sitzungen der Akkreditierungsgremien und Erstellung von INFOSEC-Empfehlungen für die SAA betreffend Akkreditierung,
    - Unterstützung bei Schulungs- und Ausbildungsmaßnahmen im INFOSEC-Bereich,
    - technische Beratung bei der Untersuchung von Zwischenfällen im INFOSEC-Bereich,

– Erstellung technischer Strategieleitlinien, um sicherzustellen, dass nur zugelassene Software verwendet wird.

FÜR DEN BETRIEB EINES IT-SYSTEMS ZUSTÄNDIGE STELLE (ITSOA)/Eigentümer des technischen SYSTEMS (TSO)

41. Die INFOSEC-Stelle delegiert zum frühestmöglichen Zeitpunkt die Verantwortung für die Implementierung und die Anwendung von Kontrollen und speziellen Sicherheitseigenschaften des SYSTEMS an die für den Betrieb des IT-SYSTEMS zuständige Stelle (ITSOA) oder gegebenenfalls an dessen Eigentümer, d.h. den Eigentümer des technischen SYSTEMS (TSO). Diese Verantwortung besteht während der gesamten Lebensdauer des SYSTEMS von der Konzeption des Projekts bis zur endgültigen Entsorgung.
42. Die ITSOA bzw. der TSO ist verantwortlich für alle Sicherheitsmaßnahmen, die als Teil des gesamten SYSTEMS konzipiert sind. Diese Verantwortung schließt die Erstellung von SecOPs ein. Die ITSOA bzw. der TSO legt die Sicherheitsnormen und -verfahren fest, die vom Lieferanten des SYSTEMS eingehalten werden müssen.
43. Die ITSOA bzw. der TSO kann gegebenenfalls einen Teil ihrer bzw. seiner Verantwortung an den für ein Projekt oder Programm zuständigen INFOSEC-Beauftragten delegieren. Die verschiedenen INFOSEC-Aufgaben können von einer einzigen Person wahrgenommen werden.

NUTZER

44. Alle Nutzer müssen sicherstellen, dass ihr Handeln die Sicherheit des von ihnen benutzten SYSTEMS nicht beeinträchtigt.

INFOSEC-SCHULUNG

45. Ausbildung und Schulung im INFOSEC-Bereich wird je nach Sachlage auf den verschiedenen Ebenen und für unterschiedliches Personal in der Hauptverwaltung, den Niederlassungen und den Anlagen der ESA oder den einzelstaatlichen Behörden angeboten.

Kapitel IV

Nichttechnische Sicherheitsmaßnahmen

SICHERHEIT DES PERSONALS

46. Die Nutzer des SYSTEMS müssen sich erfolgreich einer Sicherheitsüberprüfung unterzogen haben, die dem Geheimhaltungsgrad und Inhalt der in ihrem jeweiligen SYSTEM verarbeiteten Informationen entspricht, und müssen hierfür einen berechtigten Informationsbedarf haben. Der Zugang zu bestimmten Einrichtungen oder Informationen, die für die SYSTEME sicherheitsrelevant sind, erfordert eine besondere Ermächtigung, die gemäß den einschlägigen nationalen Vorschriften erteilt wird.
47. Die SAA benennt alle sicherheitskritischen Arbeitsplätze und legt fest, welcher Sicherheitsüberprüfung und Überwachung sich alle Personen an diesen Arbeitsplätzen unterziehen müssen, wobei gegebenenfalls die Auswirkungen der Zusammenstellung von Informationen zu berücksichtigen sind.
48. SYSTEME werden so spezifiziert und konzipiert, dass die Zuweisung von Aufgaben und Zuständigkeiten an das Personal erleichtert wird und dass vermieden wird, dass eine einzige Person umfassende Kenntnis oder Kontrolle über die für die Systemsicherheit entscheidenden Punkte erhält. Damit wird bezweckt, dass für eine Änderung oder absichtliche Schädigung des SYSTEMS oder Netzes eine Absprache zwischen zwei oder mehr Personen erforderlich wäre.

MATERIELLE SICHERHEIT

49. IT-Umgebungen und Umgebungen von dezentralen Terminals bzw. Datenstationen (gemäß den Nummern 31 und 32), in denen als „ESA VERTRAULICH“ und höher eingestufte Informationen mit informationstechnischen Mitteln verarbeitet werden oder in denen der Zugriff auf solche Informationen grundsätzlich möglich ist, werden je nach Sachlage als ESA-Sicherheitsbereiche der Kategorie I oder II bzw. gemäß deren einzelstaatlichen Entsprechungen eingestuft.
50. IT-Umgebungen und Umgebungen von dezentralen Terminals bzw. Datenstationen, in denen die Sicherheit des SYSTEMS beeinflusst werden kann, dürfen nicht mit nur einem Befugten besetzt werden.

KONTROLLE DES ZUGANGS ZU EINEM SYSTEM

51. Alle Informationen und jegliches Material, das die Kontrolle des Zugangs zu einem SYSTEM ermöglicht, werden durch Vorkehrungen geschützt, die dem höchsten Geheimhaltungsgrad und der Kategorie von Informationen, zu denen sie Zugang gewähren könnten, entsprechen.

52. Informationen und Material zur Zugangskontrolle werden, wenn sie nicht mehr zu diesem Zweck verwendet werden, im Einklang mit den SAA-Verfahren und/oder nationalen Vorschriften verwahrt. Ihre letztliche Vernichtung erfolgt gemäß den Nummern 65 bis 67.

Kapitel V

Technische Sicherheitsmaßnahmen

INFORMATIONSSICHERHEIT

53. Der Urheber einer Information hat die Aufgabe, alle informationstragenden Dokumente zu identifizieren und ihnen einen Geheimhaltungsgrad zuzuordnen, unabhängig davon, ob sie als Papierausdruck oder auf einem elektronischen Datenträger vorliegen. Auf jeder Seite eines Papierausdrucks wird oben und unten der Geheimhaltungsgrad vermerkt. Jeder Ausgabe, ob als Papierausdruck oder auf einem elektronischen Datenträger, wird der höchste Geheimhaltungsgrad der zu ihrer Erstellung verarbeiteten Informationen zugeordnet. Die Betriebsart eines SYSTEMS kann den Geheimhaltungsgrad für Ausgaben dieses SYSTEMS ebenfalls beeinflussen.
54. Die ESA-Direktionen und ihre Informationsträger müssen sich mit der Problematik der Zusammenstellung einzelner Informationsbestandteile und den Schlussfolgerungen, die aus den miteinander verknüpften Bestandteilen gewonnen werden können, auseinandersetzen und entscheiden, ob die Gesamtheit der Informationen höher eingestuft werden muss oder nicht.
55. Wenn Informationen von einem SYSTEM zu einem anderen übertragen werden, werden diese Informationen bei der Übertragung und im Empfängersystem entsprechend dem ursprünglichen Geheimhaltungsgrad und der ursprünglichen Kategorie geschützt.
56. Die Behandlung aller elektronischen Datenträger muss dem höchsten Geheimhaltungsgrad der gespeicherten Informationen bzw. der Datenträger-Kennzeichnung entsprechen; elektronische Datenträger müssen jederzeit angemessen geschützt werden.
57. Wiederverwendbare elektronische Datenträger, die zur Speicherung von ESA-Verschlusssachen verwendet werden, behalten den höchsten Geheimhaltungsgrad bei, für den sie jemals verwendet wurden, bis diese Informationen ordnungsgemäß herabgestuft worden sind oder der Geheimhaltungsgrad aufgehoben wurde und der Datenträger entsprechend neu eingestuft beziehungsweise der Geheimhaltungsgrad aufgehoben oder der Datenträger nach einem von der SAA zugelassenen Verfahren vernichtet wurde (siehe Nummern 65 bis 67).

KONTROLLE UND NACHVOLLZIEHBARKEIT IN BEZUG AUF INFORMATIONEN

58. Der Zugriff auf Informationen, die als „ESA GEHEIM“ und höher eingestuft sind, wird automatisch („audit trails“) oder manuell protokolliert und dokumentiert. Die Protokolle werden im Einklang mit diesen Sicherheitsvorschriften aufbewahrt.
59. ESA-Verschlusssachen, die als Ausgaben innerhalb der IT-Umgebung vorliegen, können als eine einzige Verschlusssache behandelt werden und brauchen nicht registriert zu werden, sofern sie in geeigneter Weise identifiziert, mit dem Geheimhaltungsgrad gekennzeichnet und angemessen kontrolliert werden.
60. Für die Fälle, in denen ein SYSTEM, in dem ESA-Verschlusssachen verarbeitet werden, Ausgaben erstellt und diese Ausgaben aus einer IT-Umgebung in die Umgebung von dezentralen Terminals bzw. Datenstationen übermittelt werden, werden von der SAA zu genehmigende Verfahren festgelegt, um die Ausgabe an den dezentralen Standorten zu kontrollieren. Für Informationen, die als „ESA GEHEIM“ oder höher eingestuft sind, beinhalten diese Verfahren besondere Anweisungen für die Nachvollziehbarkeit in bezug auf diese Informationen.

BEHANDLUNG UND KONTROLLE VON AUSTAUSCHBAREN ELEKTRONISCHEN DATENTRÄGERN

61. Alle austauschbaren elektronischen Datenträger, die als „ESA VERTRAULICH“ und höher eingestuft sind, werden als Material angesehen und unterliegen den allgemeinen Regeln. Die Identifizierung und Kennzeichnung des Geheimhaltungsgrades muss an das besondere physische Erscheinungsbild der Datenträger angepasst werden, sodass diese eindeutig erkannt werden können.
62. Die physische Entfernung von in elektronischer Form aufbewahrten ESA-Verschlusssachen aus der Hauptverwaltung, den Niederlassungen und den Anlagen der ESA muss gemäß den von der SAA genehmigten Verfahren erfolgen.
63. Die Nutzer sind dafür verantwortlich, dass ESA-Verschlusssachen auf Datenträgern gespeichert werden, die korrekt mit dem Geheimhaltungsgrad gekennzeichnet sind und angemessen geschützt werden. Um sicherzustellen, dass die Speicherung von Informationen auf elektronischen

Datenträgern für alle ESA-Geheimhaltungsgrade im Einklang mit diesen Sicherheitsvorschriften erfolgt, werden entsprechende Verfahren festgelegt.

FREIGABE UND VERNICHTUNG VON ELEKTRONISCHEN DATENTRÄGERN

64. Elektronische Datenträger, die zur Speicherung von ESA-Verschlusssachen verwendet werden, können nach einem von der SAA zu genehmigenden Verfahren herabgestuft oder freigegeben werden.
65. Elektronische Datenträger, die als „ESA GEHEIM“ und höher eingestufte Informationen enthalten haben, dürfen nicht freigegeben oder wiederverwendet werden.
66. Können elektronische Datenträger nicht freigegeben oder wiederverwendet werden, sind sie nach dem obengenannten Verfahren zu vernichten.

KOMMUNIKATIONSSICHERHEIT

67. Wenn ESA-Verschlusssachen elektromagnetisch übermittelt werden, werden besondere Maßnahmen zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit solcher Übermittlungsvorgänge ergriffen. Die SAA legt die Anforderungen an den Schutz von Übermittlungsvorgängen fest, der sich nach den Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit richtet.
68. Wenn zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von ESA-Verschlusssachen kryptographische Produkte verwendet werden sollen, müssen sie vorher von einer entsprechend qualifizierten Stelle eines ESA-Mitgliedstaats evaluiert und zugelassen werden.
69. Während der Übermittlung wird die Vertraulichkeit von als „ESA GEHEIM“ und höher eingestuften Informationen durch kryptographische Methoden oder Produkte geschützt, die vom Rat der ESA auf Empfehlung des ESA-Sicherheitsausschusses zugelassen worden sind. Während der Übermittlung wird die Vertraulichkeit von Informationen des Geheimhaltungsgrades „ESA VERTRAULICH“ oder „ESA NUR FÜR DEN DIENSTGEBRAUCH“ durch kryptographische Methoden oder Produkte geschützt, die entweder vom Generaldirektor auf Empfehlung des ESA-Sicherheitsausschusses oder von der NSA/DSA eines Mitgliedstaats zugelassen worden sind.
70. Detaillierte Regeln für die Übermittlung von ESA-Verschlusssachen werden in besonderen Sicherheitsanweisungen festgelegt, die vom Generaldirektor auf Empfehlung des ESA-Sicherheitsausschusses erlassen werden.
71. Unter außergewöhnlichen Betriebsbedingungen können Informationen der Geheimhaltungsgrade „ESA NUR FÜR DEN DIENSTGEBRAUCH“, „ESA VERTRAULICH“ und „ESA GEHEIM“ als Klartext übermittelt werden, sofern dies in jedem einzelnen Fall vom Leiter des ESA-Sicherheitsbüros ausdrücklich genehmigt und ordnungsgemäß registriert wird. Solche außergewöhnlichen Bedingungen sind gegeben
    a) während einer drohenden oder aktuellen Krisen-, Konflikt- oder Kriegssituation und
    b) wenn die Schnelligkeit der Zustellung von vordringlicher Bedeutung ist und keine Verschlüsselungsmittel verfügbar sind, und wenn davon ausgegangen wird, dass die übermittelte Information nicht rechtzeitig dazu mißbraucht werden kann, Vorgänge negativ zu beeinflussen.
72. Ein System muß in der Lage sein, bei Bedarf den Zugriff auf ESA-Verschlusssachen an einzelnen oder allen seiner dezentralen Datenstationen bzw. Terminals zu verweigern, und zwar entweder durch eine physische Abschaltung oder durch spezielle, von der SAA genehmigte Softwarefunktionen.

SICHERHEIT DER INSTALLATION UND SICHERHEIT VOR ABSTRAHLUNG

73. Die Erstinstallation von SYSTEMEN und nachfolgende größere Änderungen werden so geregelt, dass die Arbeiten von sicherheitsüberprüften Personen durchgeführt und ständig durch technisch qualifiziertes Personal überwacht werden, das zum Zugang zu ESA-Verschlusssachen des höchsten im SYSTEM voraussichtlich gespeicherten und verarbeiteten Geheimhaltungsgrades ermächtigt ist.
74. Alle Einrichtungen werden im Einklang mit den geltenden Sicherheitsvorschriften des ESA-Rates installiert.
75. SYSTEME, in denen als „ESA VERTRAULICH“ und höher eingestufte Informationen verarbeitet werden, werden so geschützt, dass ihre Sicherheit nicht durch kompromittierende Abstrahlung bedroht werden kann, wobei entsprechende Analyse- und Kontrollmaßnahmen als „TEMPEST“ bezeichnet werden.
76. TEMPEST-Maßnahmen in der Hauptverwaltung, den Niederlassungen und den Anlagen der ESA werden vom Leiter des ESA-Sicherheitsbüros als die für TEMPEST zuständige Stelle überprüft und genehmigt.

Kapitel VI

Sicherheit bei der Verarbeitung

SICHERHEITSBEZOGENE BETRIEBSVERFAHREN (SecOPs)

77. In den SecOPs werden die in Sicherheitsfragen geltenden Grundsätze, die einzuhaltenden Betriebsverfahren sowie die Zuständigkeiten des Personals festgelegt. Für die Erstellung der sicherheitsbezogenen Betriebsverfahren ist die ITSOA bzw. der TSO verantwortlich.

SOFTWARESCHUTZ UND KONFIGURATIONSMANAGEMENT

78. Der Schutz von Anwendungsprogrammen wird auf der Grundlage einer Bewertung der Sicherheitseinstufung des Programms selbst und nicht aufgrund der Einstufung der zu verarbeitenden Informationen festgelegt. Die benutzten Software-Versionen sollten in regelmäßigen Abständen überprüft werden, um ihre Integrität und korrekte Funktion sicherzustellen.
79. Neue oder geänderte Versionen einer Software sollten erst für die Verarbeitung von ESA-Verschlusssachen benutzt werden, wenn sie von der ITSOA bzw. dem TSO geprüft worden sind.

PRÜFUNG AUF DAS VORHANDENSEIN VON PROGRAMMEN MIT SCHADENSFUNKTIONEN UND VON COMPUTERVIREN

80. Die Prüfung auf das Vorhandensein von Programmen mit Schadensfunktionen und von Computerviren wird regelmäßig im Einklang mit den Anforderungen der SAA durchgeführt.
81. Alle elektronischen Datenträger, die in der Hauptverwaltung, den Niederlassungen und den Anlagen der ESA eingehen, sollten auf das Vorhandensein von Programmen mit Schadensfunktionen und von Computerviren überprüft werden, bevor sie in ein SYSTEM eingebracht werden, das vom ESA-Sicherheitsbüro genehmigte Werkzeuge und Anlagen verwendet.

WARTUNG

82. In Verträgen und Verfahrensanweisungen für die planmäßige und außerplanmäßige Wartung von SYSTEMEN, für die eine SSRS erstellt worden ist, werden Anforderungen und Vorkehrungen für den Zutritt von Wartungspersonal zu einer IT-Umgebung und für die zugehörige Wartungsausrüstung festgelegt.
83. Die Anforderungen werden in der SSRS und die Verfahren in den SecOPs präzise festgelegt. Wartungsarbeiten durch einen Auftragnehmer, die Diagnoseverfahren mit Fernzugriff erfordern, sind nur unter außergewöhnlichen Umständen und unter strenger Sicherheitskontrolle und nur nach Genehmigung durch die SAA zulässig.

Kapitel VII

AKKREDITIERUNG

84. Alle SYSTEME, für die eine SSRS erstellt werden muß, müssen von der SAA akkreditiert werden, bevor ESA-Verschlusssachen damit verarbeitet werden, und zwar auf der Grundlage der Angaben in der SSRS, in den SecOPs und in anderer relevanter Dokumentation. Teilsysteme und dezentrale Terminals bzw. Datenstationen werden als Teil aller SYSTEME akkreditiert, mit denen sie verbunden sind. Wenn ein SYSTEM sowohl von der ESA als auch von anderen Organisationen genutzt wird, nehmen die ESA und die zuständigen Sicherheitsstellen die Akkreditierung einvernehmlich vor.
85. Die Akkreditierung kann gemäß einer für das jeweilige SYSTEM geeigneten und von der SAA festgelegten Akkreditierungsstrategie durchgeführt werden.

EVALUATION UND ZERTIFIZIERUNG

86. Jedes zu beschaffende Sicherheitsprodukt (mit Ausnahme kryptographischer Produkte), das zusammen mit dem SYSTEM verwendet werden soll, sollte auf der Grundlage international anerkannter Kriterien (wie z. B. Common Criteria for Information Technology Security Evaluation, ISO 15408) entweder bereits evaluiert und zertifiziert sein oder sich in der Phase der Evaluation und Zertifizierung durch eine geeignete Evaluations- und Zertifizierungsstelle eines der Mitgliedstaaten der ESA befinden.
87. Vor der Akkreditierung werden in bestimmten Fällen die Sicherheitseigenschaften der Hardware, Firmware und Software eines SYSTEMS evaluiert und daraufhin zertifiziert, dass sie in der Lage sind, Informationen des beabsichtigten Geheimhaltungsgrades zu schützen.
88. Die Anforderungen für Evaluation und Zertifizierung werden in die Systemplanung einbezogen und in der SSRS präzise festgelegt.

89. Soweit erforderlich stellt technisch qualifiziertes und ausreichend sicherheitsüberprüftes Personal, das im Auftrag der ITSOA bzw. des TSO handelt, die Verwendung von zertifizierten Produkten sicher. Das betreffende Personal kann von einer benannten Evaluations- und Zertifizierungsstelle eines Mitgliedstaates oder deren benannten Vertretern, z. B. einem fachkundigen und ermächtigten Vertragspartner, bereitgestellt werden.

Anmerkung:

Zur Evaluation und Zertifizierung kryptographischer Produkte siehe Nummer 69.

90. Wenn die SYSTEME auf bestehenden, einzelstaatlich evaluierten und zertifizierten Computersicherheitsprodukten beruhen, können die Evaluation und die Zertifizierung vereinfacht werden (z. B. durch Beschränkung auf Integrationsaspekte).

REGELMÄSSIGE ÜBERPRÜFUNG VON SICHERHEITSEIGENSCHAFTEN ZUR AUFRECHTERHALTUNG DER AKKREDITIERUNG

91. Die ITSOA bzw. der TSO legt Verfahren für eine regelmäßige Kontrolle fest, durch die garantiert wird, dass alle Sicherheitseigenschaften des SYSTEMS noch ordnungsgemäß vorhanden sind.
92. Welche Änderungen eine neue Akkreditierung bzw. die vorherige Genehmigung durch die SAA erfordern, wird in der SSRS präzise festgelegt. Nach jeder Änderung, Instandsetzung oder Störung, die sich auf die Sicherheitseigenschaften des SYSTEMS ausgewirkt haben könnte, sorgt die ITSOA bzw. der TSO dafür, dass eine Überprüfung durchgeführt wird, um die korrekte Funktion der Sicherheitseigenschaften sicherzustellen. Die Aufrechterhaltung der Akkreditierung des SYSTEMS hängt normalerweise vom zufriedenstellenden Ergebnis dieser Überprüfung ab.
93. Alle SYSTEME, die Sicherheitseigenschaften aufweisen, werden regelmäßig von der SAA kontrolliert oder überprüft. Bei SYSTEMEN, die Informationen des Geheimhaltungsgrades „ESA STRENG GEHEIM“ oder Informationen mit zusätzlichen Kennzeichnungen verarbeiten, werden die Kontrollen mindestens einmal jährlich durchgeführt.

Kapitel VIII

Zeitlich befristete oder gelegentliche Nutzung

SICHERHEIT VON MIKROCOMPUTERN BZW. PCs

94. Mikrocomputer bzw. PCs mit eingebauten Speicherplatten (oder anderen nichtflüchtigen Datenträgern), die als Einzelrechner oder in einem Netz betrieben werden, sowie tragbare Computer (z. B. tragbare PCs und Notebook-Computer) mit eingebauten Festplatten werden im selben Sinne wie Disketten oder andere austauschbare elektronische Datenträger als Speichermedium für Informationen eingestuft.
95. Der Schutz dieser Geräte muß in bezug auf Zugang, Verarbeitung, Speicherung und Transport dem höchsten Geheimhaltungsgrad der jemals gespeicherten oder verarbeiteten Informationen entsprechen (bis zur Herabstufung oder Aufhebung des Geheimhaltungsgrades gemäß genehmigter Verfahren).

NUTZUNG VON PRIVATER IT-AUSRÜSTUNG FÜR AMTLICHE ZWECKE DES RATES

96. Die Nutzung von privaten austauschbaren elektronischen Datenträgern, privater Software und IT-Hardware mit Speichermöglichkeit (z. B. PCs und tragbare Computer) zur Verarbeitung von ESA-Verschlusssachen ist untersagt.
97. Private Hardware, Software und Speichermedien dürfen in Bereiche der Kategorien I oder II, in denen ESA-Verschlusssachen verarbeitet werden, nur mit Erlaubnis des Leiters des ESA-Sicherheitsbüros verbracht werden. Diese Erlaubnis darf nur in technisch begründeten Ausnahmefällen erteilt werden.

NUTZUNG VON IT-AUSRÜSTUNG EINES AUFTRAGNEHMERS ODER EINES MITGLIEDSTAATS FÜR AMTLICHE ZWECKE DES RATES

98. Die Nutzung von IT-Ausrüstung und Software eines Auftragnehmers für amtliche Zwecke des ESA-Rates kann vom Leiter des ESA-Sicherheitsbüros erlaubt werden. Die Verwendung der IT-Ausrüstung und Software eines Mitgliedstaats kann ebenfalls erlaubt werden; in diesem Fall unterliegt die IT-Ausrüstung der jeweiligen Bestandskontrolle der ESA. Wenn die IT-Ausrüstung zur Verarbeitung von ESA-Verschlusssachen verwendet werden soll, wird in jedem Fall die zuständige SAA konsultiert, damit die INFOSEC-Aspekte, die auf die Nutzung dieser Ausrüstung anwendbar sind, angemessen berücksichtigt und umgesetzt werden.

ABSCHNITT XII
WEITERGABE VON ESA-VERSCHLUSSSACHEN AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN

GRUNDSÄTZE FÜR DIE WEITERGABE VON ESA-VERSCHLUSSSACHEN

1. Über die Weitergabe von ESA-Verschlusssachen an Drittstaaten oder internationale Organisationen beschließt der ESA-Rat nach Maßgabe
   – von Art und Inhalt dieser Verschlusssachen;
   – des Grundsatzes „Kenntnis nur wenn nötig“;
   – der Vorteile für die ESA.

Der Mitgliedstaat, aus dem die ESA-Verschlusssache stammt, die weitergegeben werden soll, wird um Zustimmung ersucht. Aus einem Mitgliedstaat stammende ESA-Verschlusssachen dürfen nur mit Zustimmung des Urhebers oder, falls dieser nicht mehr ermittelt werden kann, mit Zustimmung des zuständigen ESA-Gremiums weitergegeben werden.

2. Einschlägige Beschlüsse werden von Fall zu Fall gefaßt und richten sich nach
   – dem gewünschten Maß an Zusammenarbeit mit den betreffenden Drittstaaten oder internationalen Organisationen;
   – deren Vertrauenswürdigkeit, die nach dem Geheimhaltungsgrad, der für die diesen Staaten oder Organisationen anvertrauten ESA-Verschlusssachen vorgesehen würde, und nach der Vereinbarkeit der dort geltenden Sicherheitsvorschriften mit denen der ESA zu bemessen ist. Der Sicherheitsausschuss der ESA gibt dazu für den Rat ein technisches Gutachten ab.
3. Der Entwurf der Vereinbarungen über Sicherheitsverfahren oder der betreffenden Abmachungen ist vom Sicherheitsausschuß zu billigen, bevor er dem ESA-Rat zur Beschlußfassung unterbreitet wird.

ABSCHNITT XIII
INDUSTRIELLE SICHERHEIT

Allgemeine Grundsätze

1. Dieser Abschnitt behandelt die besonderen Sicherheitsaspekte von Industrietätigkeiten im Zusammenhang mit der Aushandlung und Vergabe von als Verschlußsache eingestuften ESA-Verträgen (d.h. Verträge, die den Umgang mit geheimhaltungsbedürftigen Informationen nach dem ESA-Sicherheitsübereinkommen erfordern) und deren Durchführung durch industrielle Einrichtungen, wozu auch die Weitergabe von ESA-Verschlusssachen während der Angebotserstellung und den Verhandlungen vor der Vertragsvergabe gehört.
2. Alle Einrichtungen, die an industriellen Tätigkeiten mit Zugang zu Informationen des Geheimhaltungsgrads „ESA VERTRAULICH“ und/oder „ESA GEHEIM“ teilnehmen, müssen einen Sicherheitsbescheid für Einrichtungen (FSC) besitzen. Ein FSC wird von einer NSA/DSA erteilt, um zu bestätigen, dass eine Einrichtung unter dem Gesichtspunkt der Sicherheit einen angemessenen Schutz für ESA-Verschlusssachen eines festgelegten Geheimhaltungsgrads oder darunter bieten und gewährleisten kann und sein Personal, das Zugang zu ESA-Verschlusssachen haben muß, ordnungsgemäß sicherheitsüberprüft und über die Sicherheitsanforderungen der ESA, die bei der Durchführung der als Verschlußsache eingestuften ESA-Verträge zu beachten sind, belehrt wurde.
3. Die ESA bestimmt in Zusammenarbeit mit ihren Mitgliedstaaten die schutzbedürftigen Bereiche bzw. Teile eines ESA-Programms. Der ESA-Sicherheitsausschuß und das zuständige nachgeordnete ESA-Gremium empfehlen dem ESA-Rat die für den jeweiligen Bereich oder Teil des Programms vorzusehende Sicherheitseinstufung zur Genehmigung.
4. Vor der Weitergabe von Informationen des Geheimhaltungsgrads „ESA VERTRAULICH“ und/oder „ESA GEHEIM“ an einen Auftragnehmer, möglichen Auftragnehmer oder Unterauftragnehmer muß die NSA/DSA
   a. sich vergewissern, dass der bzw. die Auftragnehmer, möglichen Auftragnehmer oder Unterauftragnehmer und ihre Einrichtung(en) in der Lage sind, die Informationen angemessen zu schützen;
   b. den betreffenden Einrichtungen einen Sicherheitsbescheid für Einrichtungen (FSC) erteilen;

c. allen Personen, die zur Erfüllung ihrer dienstlichen Pflichten Zugang zu Informationen des Geheimhaltungsgrads „VERTRAULICH“ und/oder „GEHEIM“ haben müssen, eine Sicherheitsunbedenklichkeitsbescheinigung (PSC) erteilen;

d. sicherstellen, dass nur Personen, die zur Durchführung der ESA-Tätigkeiten Kenntnis von ESA-Verschlusssachen haben müssen, Zugang zu diesen erhalten;

e. auf Ersuchen des ESA-Sicherheitsbüros oder eines Mitgliedstaates einer Einrichtung einen FSC erteilen, damit sie ein Angebot für einen als Verschlußsache eingestuften Vertrag oder Untervertrag der ESA einreichen, Verhandlungen hierüber führen oder einen solchen Vertrag oder Untervertrag durchführen kann;

f. dem ESA-Sicherheitsbüro oder einem Mitgliedstaat auf Ersuchen für Personen mit Sicherheitsverantwortung die Erteilung einer PSC zusichern, damit sie an der Durchführung eines als Verschlußsache eingestuften ESA-Vertrags, der möglicherweise auch internationale Besuche umfaßt, teilnehmen können;

g. Maßnahmen im Hinblick auf die nach den Nummern 26 bis 40 dieses Abschnitts zu treffenden besonderen Vorkehrungen in Beförderungsfragen ergreifen;

h. sicherstellen, dass für jede Einrichtung, in der ESA-Verschlusssachen verwendet werden sollen, Sicherheitsbeauftragte ernannt werden, damit die Verantwortlichkeiten für den Schutz der ESA-Verschlusssachen wirksam wahrgenommen werden. Die Sicherheitsbeauftragten sind dafür verantwortlich, dass der mit einem Vertrag verbundene Zugang zu ESA-Verschlusssachen auf diejenigen Personen beschränkt bleibt, die hierfür angemessen sicherheitsüberprüft wurden und von ihnen Kenntnis haben müssen.

5. Die zuständigen Behörden der Mitgliedstaaten ermitteln in allen Fällen, in denen bekannt wird oder Anlaß zu dem Verdacht besteht, dass ESA-Verschlusssachen, die im Rahmen eines ESA-Vertrags bereitgestellt oder hervorgebracht wurden, verloren gegangen sind, Unbefugten zur Kenntnis gelangten oder an sie weitergegeben wurden. Jede NSA/DSA hält die in Abschnitt X für solche Ermittlungen festgelegten Anforderungen ein.

Sicherheitsanforderungen für als Verschlußsache eingestufte ESA-Verträge

6. Die vom ESA-Rat für die Programme genehmigten Durchführungsvorschriften enthalten eine Sicherheitsanweisung für Vorhaben (PSI) mit Sicherheitsnormen, die nicht weniger streng als die Auflagen in diesem Abschnitt sein dürfen.

7. Die PSI wird dem Hauptvertrag als Anlage beigefügt. Ein „Einstufungsleitfaden für VS-Vorhaben“ ist Bestandteil der PSI. Alle als Verschlußsache eingestuften Unterverträge der ESA enthalten den Einstufungsleitfaden für VS-Vorhaben oder mindestens eine „Geheimschutzklausel“ (SAL), die die als Verschlußsache eingestuften Teile des Untervertrags festlegt. Die PSI und/oder SAL bilden das für die Sicherheit des Vertrags maßgebliche einheitliche Dokument. Diese Sicherheitsbestimmungen müssen mit den vorliegenden Sicherheitsvorschriften der ESA übereinstimmen und mit den nationalen Gesetzen und sonstigen Rechtsvorschriften der Mitgliedstaaten, in die der Vertrag vergeben wird, vereinbar sein.

8. Alle Verträge müssen die von den zuständigen Gremien der ESA genehmigen „Sicherheitsklauseln der ESA für als Verschlußsache eingestufte Verträge“ enthalten.

9. Für alle als „ESA VERTRAULICH“ und/oder „ESA GEHEIM“ eingestuften Verträge teilt der Hauptauftragnehmer der NSA/DSA des Mitgliedstaates, in dem die Einrichtung, an die der Vertrag vergeben wurde, angesiedelt oder eingetragen ist, mit, dass dieser Einrichtung zusammen mit dem Vertrag ein Einstufungsleitfaden oder eine Geheimschutzklausel (SAL) übermittelt worden ist.

10. Die Sicherheitseinstufung für mit etwaigen Unterverträgen verbundene Informationen wird nach dem Einstufungsleitfaden für VS-Vorhaben festgelegt.

11. Der Hauptauftragnehmer und seine Unterauftragnehmer werden unter Androhung der Kündigung ihres Vertrags verpflichtet, alle von der ESA und/oder den NSA/DSA vorgeschriebenen Maßnahmen zum Schutz der ESA-Verschlusssachen, die von dem Auftragnehmer hervorgebracht oder ihm anvertraut werden oder in von ihm hergestellte Gegenstände eingehen, zu ergreifen.

12. Die Auftragnehmer und ihre Unterauftragnehmer haben die ihnen in diesen Sicherheitsvorschriften auferlegten Verpflichtungen einschließlich der Wahrung der Vertraulichkeit von Verschlusssachen auch nach der Kündigung oder Beendigung eines als Verschlußsache eingestuften ESA-Vertrags einzuhalten.[5]

Placing of ESA classified contracts involving ESA information classified CONFIDENTIAL or SECRET

13. ESA classified contracts will be placed according to the policies established by ESA.
14. The prime contractor, if duly authorised by ESA, may negotiate subcontracts with other contractors, i.e., subcontractors. The prime contractor will be responsible for all subcontracting activities.
15. The following general principles will be observed in connection with the security classification requirements of ESA classified contracts:
    a) the determination of classification levels is the responsibility of the originator of the information;
    b) classifications should apply only to those aspects of a contract that must effectively be protected and such classifications should be strictly related to the degree of protection required;
    c) a compilation of information from more than one source will require co-ordination of the sources in the determination of the appropriate ESA classification level;
    d) provisions should be made for the downgrading and declassification as soon as it is possible;
    e) changes in the level of classification should be made only with the prior consent of the originator.

[5] Anmerkung des Übersetzers:
Der deutsche Wortlaut ab Nummer 13 wird nachgereicht, sobald die amtliche deutsche Übersetzung der zugrunde liegenden NATO-Vorschriften vorliegt.

Die Bundesregierung hat beschlossen, dem Nationalrat vorzuschlagen, anlässlich der Genehmigung des Staatsvertrages gemäß Art. 49 Abs. 2 B-VG zu beschließen, dass die **französische Sprachfassung** dadurch kundzumachen ist, dass sie zur öffentlichen Einsichtnahme im Bundesministerium für auswärtige Angelegenheiten aufliegt.

Daran anknüpfend wurde mit Rücksicht auf eine sparsame und zweckmäßige Verwaltung gemäß § 23 Abs. 2 GOG-NR von der Vervielfältigung und Verteilung dieser Sprachfassung Abstand genommen.

Die gesamte Regierungsvorlage liegt in der Parlamentsdirektion zur Einsicht auf.