OCCAR Management Procedure

Title:	**OCCAR Security Regulations**
Number:	OMP 11 Date: 13/06/17
Computer Ref:	OMP 11_OCCAR Security Regulations_Issue9_20170613
Current status:	Issue 9
Contact address:	Central Office, OCCAR-EA Bonn Email: questions@occar.int

Approved for issue:	OCCAR File Ref: CO/PMSD/2017/00178

This document replaces: OMP 11 – Issue 8 dated 04/12/14

Record of changes

Date	Issue	Changes
14/02/05	1	Initial issue
13/09/06	2	Editorial changes as requested by FR, GE and UK
01/06/07	3	Separation of forms
18/06/08	4	Amendments to para. 6 and para. 12.2; revision of para. 4; incorporation of template OMP 11-10 Security Agreement; update of Security Authorities table (Annex 1, now Annex OMP 11-A), and separation of annexes from main document.
08/03/10	5	Insert para. 12.2.3 and related template OMP 11-14, incorporation of security agreement/arrangement templates OMP 11-11 to OMP 11-13, editorial changes requested by SC, amendment of para. 7,2 and incorporation of Template OMP 11-15 Security Aspects Letter, creation of Template OMP11-15 CCI Framework Transport Plan and related forms OMP 11-17, OMP 11-18 and OMP 11-19; revision of para. 4.4.5.1; amendment of the provisions regarding RESTRICTED Information in para. 5.1, 6.1, 7.1, 11.2 and 11.10 to adapt the Italian requirements.
01/12/10	6	Amendment of para. 6.3.1 and 12.2.1, deletion of the definition of "Third Party", new provisions regarding USB memory sticks in para. 9.3.3.
04/07/13	7	Fundamental revision of main body provisions and of definitions and annexes; re-arrange sequence of para.; insert new para. on minimum standards for Personnel Security Clearances; specify procedures on access by individuals and release to third countries; revise para. on handling of OCCAR RESTRICTED; revise Annex C on handling of RESTRICTED by Contractors; reduce number of forms and rename as guidance forms; list guidance forms in new Annex D; suppress previous Annex D on destruction methods for data storage media.
10/12/14	8	Introduction of additional provisions concerning release markings in para. 3.2.1; correction of cross references in para. 6.5.2, 8.3 and 11.2; Amendment of para. 10.3.
13/06/17	9	New definitions for Facility Security Clearance, OCCAR CIS, Programme Security Instructions and Security Classification Guide; editorial changes to para. 1.1.1; insertion of para. 1.4 to introduce CIS Security as a principle; appended para. 2.1 to allow establishing Experts Working Groups; modified para. 2.2 to explicitly state OCCAR-EA Director is responsible for CIS Security within OCCAR-EA; major revision of para. 9 and para. 13. 9 changed to outline general process for Security of CIS, new annexes defined for CONFIDENTIAL/SECRET and RESTRICTED specific issues, complete revision of para.10.5.

Table of Contents

List of Definitions

Board of Supervisors (BoS)	The BoS is the highest decision-making level within OCCAR.
Breach of Security	Any non-compliance with applicable security instructions or any other knowing, wilful or negligent action, especially such action that could reasonably be expected to result in loss, compromises or unauthorised disclosure of Classified Information or cause damage to the interests of OCCAR, its Member States or any other State participating in an OCCAR Programme.
Classified Information	Classified Information means any information, Document or Material the unauthorised disclosure of which could cause prejudice to the interests of OCCAR, its Member States or any other State participating in an OCCAR Programme, whether such information originates within OCCAR or is received from its Member States or from States participating in an OCCAR Programme and which has been so designated and marked with a security classification. Classified Information may include information provided by any other state or International Organisation for purposes of the Programme.
Classified Background Information	Classified Information not generated in the performance of an OCCAR Programme.
Classified Foreground Information	Classified Information generated in the performance of an OCCAR Programme.
Classified Contract	Mutually binding written agreement obligating a Contractor or Sub-Contractor to furnish supplies or services in relation with an OCCAR Programme and that either shall require access to Classified Information by the Contractor or where Contractor personnel might have access. This includes development and manufacturing of any Material and item, software, equipment, subsystem, component or special tooling where such information is being used or generated. It also includes supplies/services where Contractor personnel perform their work on the premises of a contracting facility and where they either have or might have access to Classified Information as described above. The security requirements for placing a "Classified Contract" are also applicable to all phases of pre-contract activity, including solicitation (bids, quotations, and proposals), pre-contract negotiations or post-contract activity requiring access to Classified Information by a Contractor / Sub-Contractor.

Compromise of Classified Information	Any disclosure of Classified Information to an unauthorised person.
Contractor	Any person or legal entity awarded an OCCAR Classified Prime Contract under the provisions of OCCAR Security Regulations, e.g. consultants, private companies.
Contracting Entity	Entity letting a Contract or Sub-Contract.
Controlled Cryptographic Item (CCI)	Approved hardware and software systems and equipment used for secure transmission and processing of Classified Information in communication and information systems requiring distribution control and being subject to specific procedures for handling and transfer.
Courier	An appropriately security cleared and authorised government representative, OCCAR-EA Staff Member or employee of a Contractor/Sub-Contractor approved to hand-carry Classified Information to its destination.
Designated Security Authority (DSA)	The security authority approved by national authorities to be responsible for the implementation of and compliance with the applicable security regulations and Programme Security Instructions (PSI) within Government establishments and / or industrial facilities.
Document	Any recorded information regardless of its physical form or characteristics, e.g. written or printed matter, (letter, drawings, plan), computer storage media (fixed disc, diskettes, chip, magnetic tape, CD), photographs and video recordings, optical or electronically signal / message and reproductions of them.
Downgrading	Downgrading means a reduction in the level of classification.
Declassification	Declassification means the removal of any classification.
Facility Security Clearance (FSC)	Confirmation issued by a NSA/DSA certifying that a facility under its security oversight has, in accordance with national security laws and regulations, the capability to handle and, if appropriate, store Classified Information up to a certain level and has the requisite security cleared personnel for access to such Classified Information.
Government-to-Government Channels	Transfers of Classified Information approved by NSA's / DSA's through official channels such as diplomatic or military pouch or through other channels approved by the NSA's / DSA's involved.
Material	Any item or substance from which information can be derived. This includes Documents, as defined above, equipment or weapons. Small-sized Material in principal means computer storage media and portable electronically components.
National Security Authority (NSA)	Government authority having overall responsibility for the security of Classified Information.
Need-to-Know	A determination made by an authorised holder of information that a prospective recipient has a requirement for access to, knowledge of, or possession of the information in order to accomplish a designated and approved task involving the Classified Information required to be accessed.
OCCAR	European organisation for joint armament co-operation named "Organisation Conjointe de Coopération en Matière d'Armement" (OCCAR). OCCAR consists of the Board of Supervisors (BoS) and the Executive Administration.
OCCAR CIS	Any Communication or Information System (CIS) that intends to store, forward or process OCCAR Classified Information.

OCCAR Courier Certificate	Document provided to an individual appointed to carry a classified consignment according to the provisions of para. 7.4.3, which certifies that the bearer is authorised to carry the identified classified consignment and indicates details, schedule and route of the travel.
OCCAR-EA Establishment	Buildings, offices and other premises housing OCCAR-EA Central Office or OCCAR-EA Programme Divisions located in OCCAR Member States.
OCCAR Executive Administration (OCCAR-EA)	Standing executive body of OCCAR headed by the OCCAR-EA Director responsible for the day-to-day management in accordance with regulations adopted by the Board of Supervisors (BoS). The EA comprises the Central Office (OCCAR Headquarters) and OCCAR-EA Programme Divisions whether co-located with the Central Office or located in OCCAR Member States.
OCCAR Member States	The OCCAR Member States are those European States, which are parties to the Convention on the establishment of OCCAR.
OCCAR Programme	Armaments Programme, project or any other initiatives, e.g. Technical Demonstrator Projects and related contractual pre-activities, managed by OCCAR-EA.
Originator	The State or International Organisation under whose authority or on whose behalf information has been classified.
(Programme) Participating States	States participating in an OCCAR Programme and member of the relevant Programme Board.
Personnel Security Clearance (PSC)	A determination by an NSA/DSA that an individual is, in accordance with national security laws and regulations considered suitable to access Classified Information up to a certain security classification level.
Programme Board (PB)	The OCCAR BoS consisting of the representatives of the OCCAR Member States participating in the Programme together with the Non-OCCAR Member States represented by their Ministers of Defence or the delegates of their Ministers of Defence.
Programme Committee (PC)	The PC consists of a delegate from each Programme Participating State and on behalf of the PB is responsible for supervising the running of the Programme by monitoring and approving major Programme activities, including security aspects of the Programme.
Programme Security Instruction (PSI)	The Document produced by OCCAR-EA in coordination with and approval of the Programme Participating States' NSAs/DSAs and other competent national authorities where appropriate. The PSI shall describe the compulsory security provisions required for the performance of an OCCAR-managed Programme (or during its integration into OCCAR), including details of classification, marking, handling, processing, safeguarding, releasing and transmission of Programme related Classified Information or Material. The PSI shall include the Security Classification Guide(s) and may also include a transportation plan etc. The provisions of a PSI supplement the OCCAR Security Regulations and/or national security laws and regulations.
Registry Control Officer / Personnel	Nominated OCCAR-EA staff members responsible for the management of Classified Registries or Archives established at OCCAR-EA premises.

Security Classification Guide (SCG)	The Document produced by OCCAR-EA in coordination with and approval of the Programme Participating States' competent national authorities and issued to the Programme Participants as part of to the Programme Security Instruction. The SCG shall determine the classified aspects of the Programme and the specific security classifications to be allocated to them.
Security Committee (SC)	The Security Committee consists of nominated national representatives of the NSA's/DSA's of OCCAR Member States and is chaired by one of those representatives. It is responsible directly to the BoS for considering all aspects of the security of Classified Information related to OCCAR.
Security Aspects Letter (SAL)	Document identifying the security requirements or those elements requiring security protection for an OCCAR Classified Contract.
Sub-Contractor	Any person or legal entity awarded an OCCAR Classified Sub-Contract under the provisions of OCCAR Security Regulations.

Related Forms and Templates

Form OMP 11-01	OCCAR Courier Certificate – Version I
Form OMP 11-02	OCCAR Courier Certificate – Version II
Form OMP 11-03	OCCAR FSC Information Sheet (FIS)
Form OMP 11-04	OCCAR Security Clearance Certificate
Form OMP 11-05	OCCAR Visit Request
Form OMP 11-06	Consultation Process

1. Basic Principles and Minimum Standards of Security

1.1 General

These Security Regulations lay down the basic principles and minimum standards of security to be applied by OCCAR and its Member States, so that it is assured that a common standard of protection is established for Classified Information furnished or generated in connection with OCCAR Programme activities, and uniform practices are applied.

Such Classified Information shall be distinguished either by a national classification marking or by the marking "OCCAR" together with the appropriate classification level.

OCCAR shall protect national Classified Information received from its Member States, from States participating in an OCCAR Programme or any other State, or International Organisation on the basis of the provisions of these regulations.

OCCAR Member States' Government establishments and Contractors shall protect national Classified Information furnished to them in connection with an OCCAR Programme in accordance with applicable national security laws and regulations.

1.1.1 Principles of Security in OCCAR

The principal objectives of security are to maintain the confidentiality of information by:

a) safeguard Classified Information from espionage, compromise or unauthorised disclosure;

b) safeguard important installations housing Classified Information from sabotage and malicious wilful damage;

c) in the event of failure, assess the damage caused, limit its consequences and adopt the necessary remedial measures.

1.2 Personnel Security

1.2.1 Personnel Security Clearances

All persons who require access to information classified CONFIDENTIAL or SECRET must be appropriately security cleared by their respective National Security Authority (NSA)/ Designated Security Authority (DSA) or where appropriate by the country of residency before such access is authorised. However, the Personnel Security Clearance (PSC) for OCCAR Staff Members and other personnel temporarily employed by OCCAR-EA shall be issued by the OCCAR Member State of which the individual is a national, conducting overseas checks, as appropriate.

When persons not having an established "Need-to-Know" are to be employed in circumstances in which they may have inadvertent access to information classified CONFIDENTIAL or SECRET (e.g. security agents, maintenance personnel and cleaners, etc.), they must first be appropriately security screened.

1.2.2 Security Instruction of Personnel

All personnel employed in positions involving access to Classified Information as stated under para. 1.2.1 above shall be thoroughly instructed on taking up employment and at regular intervals on the need for security and the procedures for accomplishing it. It is a useful procedure to require that all such personnel should certify in writing that they fully understand the security regulations relevant to their employment.

1.2.3 Security Status of Personnel

Procedures shall be established to ensure that, if adverse information becomes known concerning an individual, it is determined whether the individual is employed on classified work and the authority concerned informed.

1.2.4 Denial of Access to Classified Information

Persons, who are considered to be a security risk or those about whose loyalty or trustworthiness, are in reasonable doubt may be denied access to information classified CONFIDENTIAL or SECRET until the appropriate NSA/DSA has reviewed their security clearance.

1.3 Physical Security

OCCAR Member States and OCCAR-EA Establishments shall establish a system of physical security measures in order to provide a common degree of protection consistent with the security classification of the OCCAR information to be protected against unauthorised disclosure or loss.

All holders of OCCAR Classified Information shall meet the minimum standards for protection of OCCAR Classified Information as described in para. 6.

1.4 Communication and Information System Security

OCCAR Member States and OCCAR-EA Establishments that intend to store, forward or process OCCAR Classified Information in electronic form shall first undertake measures to manage Communication and Information System (CIS) Security aspects. The CIS Security measures to be applied shall be consistent with the security classification of the OCCAR Classified Information requiring protection.

To ensure a common degree of protection is obtained, all CIS handling OCCAR Classified Information shall meet the minimum standards as described in para. 9, Annex OMP 11-E and Annex OMP 11-F.

1.5 Classified Information Entrusted to Contractor Facilities or Consultants

The common levels of protection prescribed by these Security Regulations shall be equally applied to Contractor personnel and facilities outside government service or OCCAR-EA holding Classified Information, e.g. companies, consultants.

1.6 Release of Classified Information to Non-Programme Participating States

Classified Information shall only be released to States not participating in a given OCCAR Programme with the prior written consent of the Originator or of all

Programme Participating States, as appropriate, following the additional requirements and procedures as detailed in para. 10.

1.7 Threat Assessments and support to OCCAR Bodies

In accordance with their national legislation the responsible security authorities of OCCAR Member States shall provide to the OCCAR-EA Director or to his designated security organisation any intelligence or general information to allow threat-assessments to be made by OCCAR-EA to enable it to take the necessary precautions and actions regarding the protection of Classified Information concerning the:

a) physical security measures for protection of Classified Information for OCCAR-EA installations housing such information;

b) appointment and continued employment of OCCAR-EA staff providing access to Classified Information or installations housing Classified Information.

c) CIS security measures for protection of Classified Information OCCAR-EA shall refer to host nations for providing assistance and guidance in the fields of physical protection of OCCAR-EA Establishments and Classified Information held therein.

1.8 Handling of Non-OCCAR Classified Information

Classified Information provided to OCCAR by OCCAR Member States or a non-OCCAR Member State or an International Organisation on the basis of an appropriate Security Agreement/Arrangement with OCCAR shall be handled and protected in accordance with the provisions of these Agreements/Arrangements and the OCCAR Security Regulations.

2. Organisation of Security within OCCAR

2.1 OCCAR Security Committee

The OCCAR Security Committee (SC) is established in accordance with Article 7 of the OCCAR Security Agreement to consider all aspects of security of Classified Information related to OCCAR. The Terms of Reference are set out in Annex OMP 3-E.

2.2 Responsibilities of the OCCAR-EA Director

The OCCAR-EA Director is responsible to the Board of Supervisors (BoS) for:

a) enforcing the provisions of the OCCAR Security Agreement;

b) applying these Security Regulations within OCCAR-EA;

c) considering security problems referred to him/her by the NSA's/DSA's of the OCCAR Member States;

d) examining questions involving changes of these Security Regulations, in close liaison with the NSA's/DSA's of the OCCAR Member States.

Within the organisation, the OCCAR-EA Director shall be responsible for:

a) coordinating all matters of security within OCCAR, in particular issuing regulations for physical and CIS security measures within the OCCAR-EA which are compliant with the provisions outlined in para. 6 and 9 respectively;

b) preparing specific Programme Security Instructions (PSIs) and Security Classification Guides (SCGs) in consultation with the NSA's/DSA's concerned;

c) requesting NSA's/DSA's of OCCAR Member States to provide security clearances for personnel employed in OCCAR-EA Establishments and keeping a record of security clearances received from the OCCAR Member States and complementary security files;

d) ensuring that access to Classified Information is limited to those personnel holding the appropriate security clearance and having a Need-to-Know for purposes on performance of OCCAR activities;

e) requesting NSA's/DSA's of OCCAR Member States to provide Facility Security Clearances for Contractors or prospective Contractors;

f) investigating or ordering an investigation into any leakage of Classified Information which, on prima facie evidence, has occurred in OCCAR–EA Establishments;

g) requesting the appropriate security authorities to initiate investigations when a breach, compromise or leakage of Classified Information appears to have occurred outside OCCAR-EA and co-ordinating the enquiries when more than one security authority is involved;

h) maintaining close liaison with all security authorities concerned in order to achieve overall co-ordination of security;

i) keeping OCCAR-EA security organisation and procedures constantly under review and, as required, preparing appropriate recommendations.

2.3 OCCAR-EA Internal Security Organisation

In order to fulfil the responsibilities mentioned in para. 2.2, the OCCAR-EA shall have an internal security organisation, which shall be equipped adequately with personnel resources.

The OCCAR-EA security organisation shall be responsible for coordinating, supervising and implementing OCCAR security measures and verification of the enforcement of Security Regulations, including personnel security regulations within the OCCAR-EA.

It shall also be responsible for the CIS and Network within OCCAR-EA and shall co-ordinate the CIS matters within OCCAR-EA in co-ordination with NSA's/DSA's concerned.

2.3.1 OCCAR-EA Security Officer

The OCCAR-EA Director is ultimately responsible for security within OCCAR-EA. To exercise day to day security the OCCAR-EA Director appoints a dedicated Security Officer.

The OCCAR-EA Security Officer advises the OCCAR-EA Director on security matters and shall always have a direct channel to the OCCAR-EA Director as necessary.

2.3.2 OCCAR-EA Programme Divisions

Each Head of a Programme Division shall be responsible for the implementation of security within his establishment.

In order to ensure proper application of all OCCAR security provisions an appropriate member of the local staff shall act as a designated security official.

2.4 Security Inspections

Periodic inspections of the security arrangements for the protection of Classified Information within OCCAR-EA shall be carried out either by the OCCAR-EA Security Officer individually or together with the NSA/DSA concerned.

3. Security Classifications, Markings and Downgrading

3.1 Levels of Classification

The following security classifications shall be applied:

a) SECRET: For information whose unauthorised disclosure would result in grave damage to the interests of OCCAR, its Member States or other States participating in OCCAR Programmes.

b) CONFIDENTIAL: For information whose unauthorised disclosure would be damaging to the interests of OCCAR, its Member States or other States participating in OCCAR Programmes.

c) RESTRICTED: For information whose unauthorised disclosure would be disadvantageous to the interests of OCCAR, its Member States or other States participating in OCCAR Programmes.

The equivalent security classifications of OCCAR and its Member States are shown in Annex OMP 11-B.

3.2 Classification Principles

Information shall be classified only when necessary.

The classification of a Document or Material shall be determined by the level of sensitivity of its contents in accordance with the definitions given under para. 3.1 above.

The responsibility for classifying information and for any subsequent downgrading or declassification rests solely with the Originator.

3.2.1 Application of Classification and Markings

Classified Foreground Information or Classified Information, which is generated in connection with any other OCCAR-EA activities, shall be marked with the respective security classification marking identified in para. 3.1 together with the prefix "OCCAR" so as to highlight that the information is subject to the security provisions outlined in these Security Regulations and is releasable in accordance with the provisions of para. 10.

Classified Programme Foreground Information shall also indicate the name of the OCCAR Programme underneath the classification marking.

Where OCCAR Classified Information is to be released to non OCCAR Member States or Non OCCAR Programme Participating States or Contractors located in such states, the information must include an explicit releasability statement such as:

OCCAR SECRET
RELEASABLE TO [insert Non-OCCAR Member State or Non-OCCAR Programme Participating States]

Where OCCAR Classified Information is to be released to an International Organisation, it must be assessed as to whether the distribution within the International Organisation must be limited to a reduced circulation, especially only to OCCAR Member States of this International Organisation which have a need-to-know. If necessary access or distribution limitations must be added to the releasability statement such as:

OCCAR SECRET
RELEASABLE TO [insert International Organisation and certain member states of this International Organisation]

In exceptional cases, where for operational reasons or for reasons of national security Programme Participating States may not wish to release among each other Classified Information generated in connection with an OCCAR Programme, national classification markings may be applied, which may be combined with National Eyes Only markings. In such case the exception shall be addressed in the PSI and the SCG.

Classified Background Information bearing national or international classification markings shall not be remarked with an OCCAR classification marking.

3.2.2 Downgrading and Declassification

Classified Information may be downgraded or declassified only with the prior permission of the Originator in writing. Holders of Classified Information may submit requests for downgrading or declassification to the Originator. Subject to a decision by the Originator holders of classified Documents to be downgraded or declassified shall ensure that recipients of the Documents are informed about the declassification or downgrading, as appropriate.

Where appropriate, entities creating a Classified Document or Material shall specify on the Documents or Material a date or period when the contents may be downgraded or declassified. Otherwise, they shall keep the Documents or Material under review to ensure that the original classification still applies.

3.3 National Eyes Only Caveats

In cases where an OCCAR Member State or a Programme Participating State provides national Classified Information CONFIDENTIAL or SECRET to an OCCAR Programme and for operational purposes or reasons of national security, require access to such information to be limited to their nationals or to nationals of specific OCCAR Programme Participating States such Classified Information shall be marked with National-Eyes-Only caveats (e.g. "XY Eyes Only").

Such Classified Information with National-Eyes-Only caveats shall not be released to OCCAR-EA.

4. Personnel Security Clearances for Access to OCCAR CONFIDENTIAL or OCCAR SECRET Information

4.1 General

Access to information classified OCCAR CONFIDENTIAL or OCCAR SECRET shall be authorised only for persons in possession of the appropriate security clearance.

4.2 Minimum Standards for Issuing a Personnel Security Clearance

The following paragraphs define the minimum criteria for assessing the loyalty, trustworthiness and reliability of an individual in order for her/him to be granted and to retain a PSC. These criteria address aspects of the character and personal circumstances of an individual, which may give rise to potential security concerns.

Although the criteria apply to the individual being cleared, where appropriate and in accordance with national legislation, a spouse's, cohabitant's or close family member's character, conduct and circumstances may also be relevant and should be taken into account when considering an individual's eligibility for a security clearance.

4.3 Security Investigation Criteria

The criteria shall be applied to determine if an individual or his/her spouse, co-habitant, and where appropriate and in accordance with national legislation, close family member:

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

b) is, or has been, an associate of spies, terrorists, saboteurs, or of individuals reasonably suspected of being such or an associate of representatives of organisations or foreign nations, including intelligence services of foreign nations, which may threaten the security of OCCAR-EA, OCCAR Member States or States participating in an OCCAR Programme, unless these associations were authorised in the course of official duty;

c) is, or has been, a member of any organisation which by violent, subversive or other unlawful means seeks the overthrow of the government of the OCCAR Member States or States participating in an OCCAR Programme, or a change in the form of government of such States;

d) is, or has recently been, a supporter of any organisation described in sub-para. (c) above, or who is, or who has recently been closely associated with members of such organisations;

e) has deliberately withheld, misrepresented or falsified information of significance, particularly of a security nature, or has deliberately lied in completing the personnel security form or during the course of a security interview;

f) has been convicted of a criminal offence, or offences indicating habitual criminal tendencies; or has serious financial difficulties or unexplained affluence; or has a history of alcohol dependence, use of illegal drugs and/or misuse of legal drugs;

g) is or has been involved in conduct, including any form of sexual misconduct, which may give rise to the risk of vulnerability to blackmail or pressure;

h) has demonstrated, by act or through speech, dishonesty, disloyalty, unreliability, untrustworthiness or indiscretion;

i) has seriously or repeatedly infringed security regulations; or has attempted, or succeeded in, unauthorised activity in respect to communication and information system(s);

j) is suffering, or has suffered, from any illness or mental or emotional condition which may cause significant defects in his judgement or reliability or may make the individual, unintentionally, a potential security risk. In all such cases competent medical advice should be sought; or

k) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations or individuals whose interests may threaten the security interests of OCCAR-EA, OCCAR Member States or States participating in an OCCAR Programme.

4.4 Minimum Investigative Requirements for Personnel Security Clearances

The initial security clearance process for access to information classified OCCAR CONFIDENTIAL and SECRET shall be based on enquiries covering at least the last 5 years, or from age 18 to the present, whichever is the shorter; and shall include the following:

a) the completion of a Personnel Security Questionnaire;

b) identity check / citizenship / nationality status – The individual's date and place of birth shall be verified and his/her identity checked. Citizenship status and/or nationality, past and present, of the individual shall be established; this shall include an assessment of any vulnerability to pressure from foreign sources; for example, due to former residence or past associations; and

c) national and local records check – A check shall be made of national security and central criminal records, where these latter exist, and/or other comparable governmental and police records for any officially recorded indication of disloyalty or unreliability. The records of law enforcement agencies with legal jurisdiction where the individual has resided or been employed for at least six months shall be checked.

The NSA/DSA or other competent security authority shall consider all available information in order to determine whether a PSC shall be granted or not. It should be noted that indications of potential vulnerability to pressure (e.g. debts or the potential vulnerability of a spouse/cohabitant/close family member) need not be a reason to deny clearance if the subject's loyalty, trustworthiness and reliability are undisputed. The NSA/ DSA or other competent security authority shall assess the risks associated with each case in order to determine whether a clearance may be granted.

Lack of coverage of any investigative shall be compensated for through other investigative means in accordance with national security rules and regulations category.

After the initial granting of a PSC and provided the individual has had unbroken service with OCCAR-EA, an OCCAR Member State's or Programme Participating State's Government establishment or a Contractor, the PSC shall be reviewed for revalidation at intervals not exceeding 10 years.

4.5 Security Clearances for OCCAR-EA Staff Members and Detached National Experts

The clearance of OCCAR-EA Staff Members and Detached National Experts shall be the responsibility of the individual's respective national government based on national security laws and regulations.

This shall result in the issue of a Security Clearance Certificate showing the level of Classified Information to which the cleared person may have access and the date of expiry, and conform to the relevant OCCAR guidance form.

NSA's/DSA's of the OCCAR Member States shall ensure that their national representatives to the BoS hold the Security Clearance.

4.6 Security Clearances for Contractor Personnel

PSCs for nationals of the OCCAR Member States residing, and requiring access to Classified Information, in their own country shall be undertaken by their NSA/DSA.

However, PSCs for nationals of the OCCAR Member States who are legally resident in the country of another OCCAR Member State and apply for a job in that country shall be undertaken by the competent security authority of that country conducting overseas checks as appropriate, and notifying the parent country.

A PSC issued by one NSA/DSA shall be accepted by the other NSA's/DSA's of the OCCAR Member States for employment involving access to Classified Information within a company in their own country.

PSCs issued by the NSA's/DSA's of OCCAR Member States shall be mutually accepted if the individual concerned applies for employment in another OCCAR Member State.

NSA's/DSA's of OCCAR Member States having issued a security clearance for an individual holding the nationality of another OCCAR Member State shall on request of other NSA's/DSA's of OCCAR Member States issue a Security Clearance Certificate for such individuals applying for a job in the requesting OCCAR Member State.

4.7 Exchange of Information Affecting the Security Status of Personnel

If any information about one of its Nationals being appointed to OCCAR-EA in a post requiring access to Classified Information or being employed with industry and for whom a PSC has been issued is received by an OCCAR Member State, which in its opinion would affect the security of OCCAR-EA or one of its Member States, that Nation shall either communicate such information to the OCCAR-EA Security Officer or withdraw that person's PSC.

Where such information has been obtained by an OCCAR Member State in respect of another OCCAR Member State or by OCCAR-EA Security Officer in respect of an OCCAR-EA Staff Member, the OCCAR Member State concerned should be advised.

4.8 Records of Access Authorisations / Personnel Security Clearances

All establishments handling information classified CONFIDENTIAL or SECRET shall maintain a record of PSCs granted for their personnel.

Each security clearance shall be verified, as the occasion demands, to ensure that it is adequate for that person's current employment.

Such records and complementary files for security cleared personnel shall be held by the responsible security officers.

5. Access to OCCAR CONFIDENTIAL or OCCAR SECRET Information

5.1 General Requirements

Access to Classified Information shall be authorised only to persons having a Need-to-Know for carrying out their duties.

Any such access to information classified CONFIDENTIAL or SECRET shall be authorised only for persons in possession of the appropriate PSC.

The provisions described hereafter apply to Government officials, OCCAR-EA Staff Members or other personnel temporarily employed by OCCAR-EA and Contractor personnel, as appropriate, who require access to information classified CONFIDENTIAL or SECRET.

5.2 Access by Individuals holding the Nationality of an OCCAR Member State

Individuals holding the nationality of an OCCAR Member State, and being employed in an OCCAR Member State, can have access to information classified OCCAR CONFIDENTIAL or OCCAR SECRET without the prior consultation with and approval of the Originator.

5.3 Access by Other Nationals

5.3.1 Access by Nationals from Programme Participating States

Individuals holding the nationality of a Programme Participating State, which is not an OCCAR Member State, and being employed in an OCCAR Member State or a Programme Participating State can have access to Programme Foreground Information classified OCCAR CONFIDENTIAL or OCCAR SECRET without the prior consultation with and the approval of the Originator.

5.3.2 Access by Nationals from Non-Programme Participating States

Individuals holding the nationality of a State that is not an OCCAR Member State nor a Programme Participating State can only have access to OCCAR Classified Information CONFIDENTIAL or SECRET after consultation with and approval of the Originator.

Access to Programme Background Information classified CONFIDENTIAL or SECRET by individuals shall require prior approval of the originating State or International Organisation.

5.3.3 Simplified Access to Classified Information

In order to simplify access to OCCAR Classified Information the Programme Participating States may agree in PSIs that the access limitations in para. 5.3.2 may be less stringent.

5.4 Consultation Process

The consultation process concerning the access to classified Information at the level of OCCAR CONFIDENTIAL or OCCAR SECRET by individuals holding the nationality of non-OCCAR or non-Programme Participating States shall be the following:

a) The NSA/DSA of the OCCAR Member State or Programme Participating State where the individual is employed shall notify and consult each other where access to OCCAR Classified Information at the level of CONFIDENTIAL or SECRET is required by individuals holding the nationality of non-OCCAR or non-Programme Participating States. OCCAR-EA shall be informed about the decision made in connection with a consultation process;

b) The information to be provided in connection with the consultation process shall be limited to the nationality of the individual concerned and the details on the Classified Information to be accessed by the individual unless the OCCAR Member State receiving the notification requires more details or other relevant information on a case by case basis;

c) The OCCAR Member States or Programme Participating State concerned shall assess and decide on whether the individual can be granted access to OCCAR Classified Information;

d) Such consultations shall be given urgent consideration with the objective of reaching a consensus within four weeks of the date of the request.

For the consultation process, OCCAR Member States shall use the relevant OMP 11 guidance form.

5.5 Access Authorisations

Access to Classified Information shall be subject to the following:

a) a PSC at the appropriate level,

b) a Need-to-Know;

c) the appropriate nationality;

d) approval has been obtained for individuals holding a nationality for which prior consultation is required.

For OCCAR-EA staff and Detached National Experts employed with OCCAR-EA and requiring access to Classified Information at the level of CONFIDENTIAL or above such access authorisation shall be given by the OCCAR-EA Corporate Management or by the respective OCCAR-EA Programme Manager, where Programme-specific Classified Information is involved.

For Contractor personnel and OCCAR Member States' Government agencies, the access authorisation shall be taken by the responsible security officials.

5.6 Security Instruction of Personnel

Persons who are required to handle information classified CONFIDENTIAL or SECRET should, on first taking up their duties and periodically thereafter, be made aware of:

a) the dangers to security arising from indiscrete conversation;

b) precautions to take in their relations with the press;

c) the threats, which may target the OCCAR-EA and its Member States;

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

6. Physical Protection of OCCAR-EA Premises and of CONFIDENTIAL or SECRET Information

6.1 Need for Protection

The objective of physical security measures is to prevent unauthorised persons from gaining access to Classified Information.

6.2 General Security Requirements

All premises (areas, buildings, offices, rooms etc.) in which Classified Information is handled or stored shall be protected by appropriate security measures.

Physical security precautions to be established for the protection of Classified Information in particular shall depend on the security classification, the physical form and the volume of the information or Material held, the locally assessed threat, which may arise from espionage, sabotage or terrorist or any other violent and/ or criminal activities, the location and construction of buildings or areas housing classified Material, the degree of other site-specific organisational or technical protective measures planned or in place, such as access controls or guarding, other relevant factors, e.g. security status of personnel or general information security measures.

Physical security measures, as a minimum, must be designed to deny surreptitious or forced entry by an intruder, deter, impede and detect actions by disloyal personnel and allow for segregation of staff in their access to Classified Information on a strict Need-to-Know-basis.

All equipment and devices used for direct or indirect protection of information classified at CONFIDENTIAL level or above (e.g. steel cabinets, shredding and copying machines, locks for doors, electronic access control systems, intrusion detection systems, alarm systems, technically security areas) must comply with OCCAR Member States' national security requirements or shall be certified by the relevant National Security Authority or Designated Security Authority, as appropriate.

OCCAR-EA should receive advice from the competent national security authorities of the OCCAR Member State hosting OCCAR-EA Establishments.

6.3 Minimum Requirements for Buildings housing Classified Information at

CONFIDENTIAL OR SECRET Level

6.3.1 Construction of Buildings

Buildings housing Classified Information and/or OCCAR-EA Establishments must be of solid construction and offer a degree of resistance to forced intrusion (brick or block, on cavity wall principles or similar construction; windows and doors of a standard equal to that of the building in its resistance to forced entry), and must also be protected against unauthorised access.

Windows at basements, ground floors or defined security areas must offer a delay and suitable degree of resistance to an intruder with a limited range of hand tools.

All other windows of buildings housing OCCAR-EA Establishments must offer a suitable degree of protection against thrown items.

Entrances and doors to buildings and underground parking facilities must offer a delay and degree of resistance to forced intrusion with a limited range of hand tools (doors of solid wood construction and/or fitted with laminated security glass in a suitable frame).

For buildings where main entrances are located close to public roads, adequate obstacles must be installed to prevent any unauthorised parking of vehicles directly in front of the building.

6.3.2 Perimeter Fences

Perimeter fences of solid metal construction must be installed around premises to include gates with proper access control for pedestrians offering a minimum of deterrence or resistance to anyone other than a determined intruder.

The outer area may be observed by guards conducting frequent random patrols who shall be able to verify incidents on the site or at the perimeter and prevent any attempt of forced entry or summon additional response forces (e.g. from local police).

6.3.3 Guarding of Buildings

The outer area of buildings housing Classified Information and/or OCCAR-EA Establishments must be observed by guards conducting frequent random patrols, who shall be able to verify incidents on the premises or at the perimeter, and prevent any attempt of forced entry or summon additional response forces (e.g. from local police).

The number and frequency of patrols shall be determined according to the locally assessed threat and security environment.

Guards may be supported by Closed Circuit Television or security lighting.

6.3.4 Access Control at Entries to Buildings and Parking Facilities

A system of access control (e.g. barriers combined with automatic access control systems) must be exercised at entrances to buildings housing Classified Information and/or OCCAR-EA Establishments and associated

parking facilities, where appropriate, allowing proper control of all individuals, who need to access the premises.

6.4 Basic Principles and Minimum Requirements for Access Control and Physical Security of Classified Information at CONFIDENTIAL or SECRET Level

6.4.1 General

Classified Information at CONFIDENTIAL or SECRET level shall be handled or stored in security areas or administrative zones with proper access control so that it can be assured that only individuals holding a security clearance of the appropriate level can have access to the Classified Information handled, displayed or stored therein.

Outside working hours or during times such areas are not occupied by authorised personnel the Classified Information must be deposited in nationally approved security containers, strong rooms or open storage areas, which shall be subject to continuous protection or periodic inspections.

Physical security precautions and technical equipment established for the protection of Classified Information shall be designed to deny surreptitious or forced entry by an intruder, deter, impede and detect actions by disloyal personnel, sufficiently delay intruders for response forces to effectively prevent an intruder from gaining access to Classified Information and allow for segregation of staff in their access to Classified Information on a strict Need-to-Know.

For OCCAR-EA Establishments such equipment must be certified by the competent NSA/DSA of the OCCAR Member State hosting the establishment.

Given sufficient time, almost any physical security measure is vulnerable to being overcome. It is therefore important to evaluate the effectiveness of both specific security measures and the overall system in terms of delay and reaction times.

Delay measures therefore shall be evaluated against the time required to gain unauthorised access.

Response measures shall be evaluated based on the time needed, from the moment the alarm is received, to mobilise the response force, to cover the distance from the mobilisation point to the facility and to access the compromised area.

6.4.2 Minimum Standards for Storage of CONFIDENTIAL or SECRET Information

Security containers or strong rooms and open storage areas when not occupied used for storage of CONFIDENTIAL or SECRET information shall be protected by one of the following methods:

a) Continuous surveillance by guards or other duty personnel holding a security clearance of the appropriate level;

b) Regular inspection of the security container by security cleared guards or duty personnel on a 24 hours basis;

c) A nationally-approved intrusion detection system or 4closed circuit video system in combination with a response force that shall, following an

alarm , arrive at the location within the timeframe an intruder would need to remove or gain access to the security container, or to force entry into a strong room.

6.4.3 Security Containers

Security containers used for storage or archiving of Classified Information at CONFIDENTIAL or SECRET level shall be designed to sufficiently delay an intruder having a limited range of hand tools at his disposal until he can be detained by response forces. Security containers must be of solid metal or steel construction and be equipped with built-in nationally approved three-position combination or similar lock.

6.4.4 Strong Rooms / Open Storage Areas

Strong rooms used for open storage of classified Documents or Material at CONFIDENTIAL or SECRET level shall meet the following standards:

a) Perimeter walls, floor and ceilings of solid construction, or where establishment of walls is not appropriate due to the size of the Material or equipment perimeter construction must be of a manner so as to provide visual evidence of unauthorized penetration;

b) Doors to be of solid construction in either wood or metal;

c) Entrance doors to be secured with a built-in nationally approved three-position combination or similar lock;

d) Windows at ground level, or where appropriate at other levels, to be constructed from, or covered with Materials, that provide protection from forced entry (e.g. laminated security glass in suitable frames or fitted with steel bars);

e) Windows to be made inoperable (e.g. by permanent sealing or with inside locking mechanism) or to be covered by an intrusion detection system, which may be combined with motion detection sensors within the area;

f) All windows be made opaque or equipped with blinds, drapes or other coverings in case windows may reasonably afford visual observation of classified Documents or Material or activities within the facility;

g) All vents, ducts and similar openings in excess of 15 x 15 centimetres that enter or pass through a strong room or open storage area to be protected with either bars, expanded metal grills, commercial metal sounds baffles, or an intrusion detection system.

Entry controls must be exercised at entrances to strong rooms by designated personnel or by an access control system allowing only security cleared and authorised personnel to access the area.

6.4.5 Security Areas and Administrative Zones

All areas, where Classified Information is generated, transmitted or displayed otherwise shall be established as security areas or administrative zones with proper entry controls.

During normal working hours such areas must be locked when not occupied.

Outside working hours Classified Information must be stored in security containers or strong rooms as described under para. 6.4.3 and 6.4.4 above.

6.4.6 Guards / Other Response Forces

When guards are used to ensure the integrity of security containers, strong rooms, open storage area or other security areas, where OCCAR Classified Information is handled or stored they must be appropriately security cleared and qualified, trained and supervised.

The response forces shall be required to provide a minimum of two persons to any point of a security disorder on the site without weakening site protection elsewhere.

Guards' response to alarms or emergency signals shall be tested and shall be within a time limit evaluated as capable of preventing an intruder's access to the Classified Information being protected.

6.4.7 Control of Keys and Combinations

Working keys for security containers, strong rooms or other security areas, housing Classified Information, as well as keys operating alarm systems used to protect such areas, shall not be taken out of office buildings.

All such keys shall be deposited in dedicated security key containers accessible to designated staff only, when not in use.

Security key containers shall be guarded or kept under permanent control by local security personnel.

Combination settings of security containers shall be committed to memory by individuals needing to know them.

Knowledge of combination settings of security containers and codes for alarm systems established for protection of security containers and security areas shall be restricted to the smallest possible number of individuals.

The record of each combination shall be kept in a separate envelope.

The keys, combinations and the envelopes shall be given security protection not less stringent than the information to which they give access.

Working and spare security keys shall be kept in separate containers unless local security environment may justify storage in a single security container.

Spare keys and a written record of each combination setting for use in an emergency shall be held in sealed opaque envelopes by the local security managers.

Combination settings for security containers shall be changed:

a) On first being taken into use;

b) Whenever a change of personnel possessing the combination occurs;

c) Whenever a compromise has occurred or is suspected, and

d) At intervals not exceeding 12 months.

6.4.8 Physical Protection of Communication and Information Systems

CIS used for processing or transmission of Classified Information shall be protected by appropriate physical security measures to ensure that only authorised persons can use them, and that Classified Information is protected and controlled as set out in para. 9.

6.4.9 Protection against Eavesdropping

Areas in which information classified SECRET is discussed regularly shall be protected against passive eavesdropping (leakage of Classified Information via insecure communications or by overhearing directly) and active audio eavesdropping (leakage of Classified Information by wired microphones, radio microphones or other implanted devices).

This may involve the soundproofing of walls, doors, floors and ceilings, technical or physical security inspection of furniture, office equipment and offices/meeting rooms carried out by competent and authorised technical experts only.

OCCAR-EA may request assistance by experts from the competent NSAs hosting OCCAR-EA Establishments.

Such areas shall be established as security areas with proper access control, and technical controls of any equipment or furniture used.

6.5 Administrative Control of Classified Information or Material at CONFIDENTIAL level or above

6.5.1 General Requirements

Registry systems shall be established in order to control the receipt, creation, accounting, handling, internal distribution, dispatching to external recipients, reproduction and destruction of Classified Information or Material at CONFIDENTIAL level or above.

In order to ease control and location of Classified Information or Material classified CONFIDENTIAL or SECRET the management of such Classified Information or Material held within a building or a closed group of buildings shall be centralised to a maximum extent unless the amount of Classified Information or Material justifies decentralised management.

6.5.2 Classified Registries and Archives

Classified Registries shall act as the main receiving and dispatching point for Classified Information or Material classified CONFIDENTIAL or SECRET and shall be operated by trained registry personnel only holding a security clearance at the appropriate level.

All incoming classified consignments as well as Documents or Material created within a given establishment containing CONFIDENTIAL or SECRET information must be forwarded to local Classified Registries in order to allow proper registering in appropriate Register Books.

Only authorised OCCAR-EA Registry Control Personnel may open the inner cover of such classified consignments and acknowledge receipt of the Documents enclosed.

Accordingly, all Documents or Material classified CONFIDENTIAL or SECRET shall be forwarded to external recipients via the Classified Registry only.

Registry Control Personnel shall be responsible for proper registration and control of all incoming or on-site produced Documents or Material of such classification, including reproduction or destruction thereof. They shall also be responsible for internal distribution and for keeping records of the location of each Document.

Classified Registries shall:

a) Ensure the physical safeguarding of all classified Documents or Material at CONFIDENTIAL or SECRET level held by the Central Registry;

b) Maintain an up-to-date record of all CONFIDENTIAL or SECRET Documents or Material held or circulating within premises for which the registry is responsible;

c) Maintain up-to-date records by name of all individuals authorized to have access to such Documents or Material held by the registry;

d) Internally distribute such classified Documents or Material only to those individuals authorized to receive it;

e) Dispatch externally such Documents or Material only addressees authorised to receive the Documents or Material;

f) Ensure proper packaging and conformity with applicable requirements for transfer/transmission;

g) Obtain receipts for all Documents or Material distributed internally or dispatched externally;

h) Ensure a notice for a change in classification, Declassification or destruction certificate is held;

i) Carry out inventories on an annual basis;

j) Ensure classified Documents or Material accounted for is physically present and contain the correct number of pages.

Classified Registries shall be established as a Security Area with a control of entry system, which shall admit only specially authorised staff to enter the area.

Classified Registries may be co-located with classified archives used for storage of Classified Information. In such a case they shall be protected in accordance with the standards set out in para. 6.4.2, 6.4.3 and 6.4.4 above.

6.5.3 Classified Registers

Classified Registers shall keep up-to-date records of the receipt, disposition and dispatching of Documents or Material and shall be maintained using appropriate register or log books.

As a minimum, the following details shall be recorded in Classified Registers:

a) Internal register/serial number and classification level;

b) Date of receipt;

c) Date of creation of Document or Material;

d) Entity having created or provided the Document/Material;

e) Subject or title;

f) Copy number;

g) Number of annexes, if appropriate;

h) Total number of pages / Material;

i) Details of internal handling (destruction, Downgrading, creation of copies, internal);

j) Details of dispatching to external recipients (date, copy number, recipient).

6.5.4 Dispatching of Classified Information to External Recipients

For any transfer of Classified Information or Material to external recipients the sending establishment shall provide an appropriate dispatch note requiring the recipient to confirm the receipt. As a minimum, such dispatch notes shall quote the serial number of the note and the details of the Classified Information or Material dispatched.

Prior to dispatching Classified Information or Material to external recipients the dispatching Classified Registry shall check with the responsible security authority whether the recipients hold a FSC at the appropriate level, in case recipients are industrial facilities.

Dispatch notes returned from external recipients of classified consignments shall be kept for 5 years.

For transfer of classified consignments via Government-to-Government channels Classified Registries shall add additional dispatch forms as required by host nations' security regulations for the first step in the Government-to-Government channel.

Classified Registries may also keep details of internal recipients or access to the Classified Information or Material.

Register books closed shall be retained for a minimum of 5 years.

Registers for Classified Information or Material may be maintained via IT systems, which have been properly approved by the responsible NSA/DSA.

6.5.5 Preparation of Classified Documents or Material

Documents or Material containing Classified Information or derivatives and reproductions thereof containing such information shall be marked to identify its classification and the entity having created the information, and as stated in PSIs or SCGs.

Material containing Classified Information must be marked in such a manner as to ensure that any recipient or viewer shall know that Classified Information of a specified level is involved.

The assigned security classification and, where appropriate, Downgrading and Declassification instructions shall be conspicuously stamped, printed, written, painted or affixed by means of a tag, sticker, decal or similar device on classified Document or Material.

For a given Document, individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures may require different classifications and shall be marked accordingly.

The classification of the Document as a whole shall be that of its most highly classified part.

Extracts from SECRET or CONFIDENTIAL Documents shall also be marked with the appropriate classification marking of the Document or component thereof (if individually classified) from which it is taken unless it is obvious that it justifies another classification. In such a case advice shall be sought from the responsible NSA/DSA or other national classification authority for determination of the correct classification.

The entity creating such Classified Information will ensure that all Documents and copies or reproductions thereof containing Classified Information at CONFIDENTIAL or SECRET level will be conspicuously stamped, typed, printed or written in bold and capital letters at the top of the front cover or cover letter, and at the top and bottom of each page indicating the overall classification of the Document.

For SECRET Documents the marking will be in red colour and for CONFIDENTIAL in black or blue colour.

Material (e.g. items of machinery, equipment) or removable computer storage media (e.g. floppy disks, compact disks, microchips) and other optical, acoustical or electronic recordings containing Classified Information shall be marked properly either on the Material itself or – if not possible – on the container holding the Material in such a manner that any recipient shall know Classified Information is involved (e.g. by affixing a tag or sticker).

6.5.6 Reproduction

Any creation of copies or reproductions from CONFIDENTIAL or SECRET Documents or data storage media containing such Classified Information shall as a whole or from parts thereof, take place under the strict observation of the Need-to-Know principle, and be subject to a prior written copy order given by the competent senior or other duly authorised staff.

Copy orders shall specify, as a minimum, the name of the person having confirmed the necessity of copies, the number of copies to be created and the date and signature of copy order.

The creation of copies from Documents (hardcopies) shall be carried out, for SECRET information, in the presence of two persons authorised to access the Material, on dedicated copy machines and in areas with proper access control.

The creation of copies shall be confirmed on appropriate certificates indicating the date and the number of copies produced and the names and signature of persons involved in the creation of copies.

Copies shall be marked with identifying reproduction copy number.

The total number of reproductions, including reproduction copy numbers shall be recorded in the respective column of the Classified Register.

Electronic copies, which need to be taken from computer data storage media or any hardcopy output containing CONFIDENTIAL or SECRET information, must be carried out on approved IT equipment as described in para. 9.

6.5.7 Destruction

Any destruction of Documents or Material classified CONFIDENTIAL or SECRET shall be subject to a prior written destruction order given by the competent senior or other duly authorised staff.

Any such destruction shall be carried out using nationally approved shredding machines or equipment in presence of an authorised second staff member only.

The destruction process shall be recorded on an appropriate destruction certificate and the destruction shall be confirmed by the same two persons. Destruction Certificates shall also be retained for a minimum of 5 years.

6.5.8 Inventory Checks

Classified Registry Control Personnel shall carry out yearly inventory checks of all Documents or Material kept under their control in order to keep updated information about the total number of CONFIDENTIAL and SECRET Documents or Material held within the respective establishment, and to check the physical presence of Documents or Material recorded in Register Books.

The results of such inventories shall be reported to the responsible security official by the end of each calendar year.

The responsible NSA's/DSA's may conduct periodic spot-checks of Classified Registries to monitor the application of the provisions set out in this Document, and to verify the continued control of CONFIDENTIAL or SECRET Documents or Material held there.

Such spot checks shall be carried out to verify:

a) Consistency with information recorded in Register Books and physical presence of Documents or Material held within the registry;

b) Physical presence of copy and destruction certificates;

c) Physical presence of signed copies of dispatch notes/receipts for Documents or Material dispatched to external recipients;

d) Evidence of tracer action taken and results thereof, in cases where such signed dispatch notes/receipts are not available.

7. Movement of OCCAR CONFIDENTIAL or OCCAR SECRET Information

7.1 General Requirements for the Movement of OCCAR CONFIDENTIAL and OCCAR SECRET Information

The provisions described hereafter apply to movement of Classified Information at the OCCAR CONFIDENTIAL and OCCAR SECRET levels, like Documents, small sized Material or large volumes of classified Material, including components or weapon systems.

Information classified CONFIDENTIAL or SECRET shall be transferred across borders by the following means:

a) Government-to-Government channels, i.e. diplomatic pouch or military channels;

b) security cleared government or company employees, or OCCAR-EA staff members acting as couriers following procedures as detailed hereafter;

c) commercial courier companies (for CONFIDENTIAL), (any Contractor planning to use commercial courier companies must first ask for prior approval from its NSA/DSA);

d) Electronic transmission by Information- and Communications Systems accredited by the competent national authority.

PSIs may further specify the requirements for transfer of Classified Information according to the needs of a given OCCAR Programme, provided they are no less stringent than these regulations.

7.2 Packaging of Documents and Small-Sized Material Classified CONFIDENTIAL or SECRET

Information classified CONFIDENTIAL or SECRET shall be moved in heavy duty, double opaque and strong cover envelopes or packaging.

The inner cover shall bear the name and addressee and be stamped with the appropriate classification and shall be enclosed in a secure outer cover.

The outer cover shall bear a designation address and a package number for receipting purposes and shall not indicate the classification of the contents or the fact that it contains Classified Information.

A locked and sealed pouch / box may be considered as the outer cover.

Only the Registry Control Officers or other authorised Registry Control Personnel may open the inner cover and acknowledge receipt of the information enclosed.

Other methods of packaging may be used provided they allow for detection of any attempt of unauthorised opening of the consignment. The consignee shall check the packaging for damage.

7.3 Movement of Information Classified CONFIDENTIAL or SECRET within OCCAR Member States

Information classified CONFIDENTIAL or SECRET shall be transferred within OCCAR Member States in accordance with national security laws and regulations.

7.4 International Movement of Information Classified OCCAR CONFIDENTIAL or SECRET

7.4.1 Movement through diplomatic channels

Information classified CONFIDENTIAL or SECRET shall normally be moved between OCCAR and the OCCAR Member States and between OCCAR Member States through Government-to-Government diplomatic bag channels.

7.4.2 Movement via commercial companies

In cases of urgency, i.e. only when the use of Government-to-Government diplomatic bag channels cannot meet the needs of OCCAR, OCCAR Classified Information at CONFIDENTIAL level may be moved via commercial courier companies, provided that the following criteria are met:

a) the courier company is located within an OCCAR Member State or Programme Participating State and has established a protective security program for handling valuable items with a signature service, including a record of continuous accountability on custody through either a signature and tally record, or an electronic tracking/tracing system;

b) the courier company shall obtain and provide to the consignor proof of delivery on the signature and tally record, or the courier must obtain receipts against package numbers;

c) the courier company must ensure that the consignment shall be delivered to the consignee prior to a specific time and date within a 24-hour-period under regular circumstances;

d) the courier company may charge a commissioner or Sub-Contractor.

However, the responsibility for fulfilling the above requirements must remain with the courier company.

With the prior agreement of the appropriate NSA's/DSA's, national Classified Information at CONFIDENTIAL level may also be transmitted via commercial courier companies provided the above criteria are met.

7.4.3 Hand-carriage of Classified Consignments

In urgent cases information classified CONFIDENTIAL or SECRET which comply with the packaging requirements as described in para. 7.2 above may be carried by hand by OCCAR-EA staff members or Government or Contractor personnel provided that:

a) the Courier holds the appropriate security clearance;

b) the Courier is aware of his responsibilities for safe custody;

c) the Courier carries a single or multi-travel Courier Certificate authorising him/her to carry the package as identified;

d) a record of the information so carried is held in the appropriate registry of the dispatching facility.

The dispatching authority / facility shall notify the receiving authority / facility about the details (e.g. reference, classification, time of arrival, name of Courier) prior to the hand-carriage taking place. The dispatching authority / facility shall also notify via its NSA/DSA the NSA/DSA of the receiving authority / facility two working days prior to the transportation.

For hand carriage of Classified Information at CONFIDENTIAL or SECRET level by OCCAR-EA staff, experts and OCCAR Member States' representatives enjoy inviolability for all their official papers and Documents while exercising their functions and in the course of hand carriage between OCCAR Member States.

7.4.4 Courier Certificates

For the international hand carriage of Classified Information by OCCAR-EA Staff members or Government Representatives or Contractor personnel at CONFIDENTIAL or SECRET level Courier Certificates shall be used.

The responsible NSA/DSA and OCCAR-EA security officials shall issue or authorise the issuing of Courier Certificates for government representatives or Contractor personnel, which should conform to the standards identified in the relevant OCCAR Courier Certificate guidance form.

7.4.5 Transportation of Items Classified CONFIDENTIAL or SECRET as FREIGHT by commercial carriers

Classified items that cannot be moved by one of the foregoing methods or where large volumes of classified Material (e.g. equipment, components of weapons) need to be moved such items may be transported as freight by security cleared or approved commercial carriers subject to the following requirements:

a) The carrier company must be approved for the transportation of Classified Material;

b) The carrier company must hold a FSC at the appropriate level, if required by national security laws and regulations;

c) Where ever possible, consignments shall be transported point-to-point;

d) The consignor and consignee are responsible for jointly organising the transport including preparing a transportation plan (see guidance Form OMP 11), and for its notification to and approval by their respective NSA/DSA prior to transportation;

e) Where appropriate the NSA's/DSA's shall advise their customs or other relevant national authorities of impending consignments and should be urged to give maximum priority to the shipment;

f) Where possible the consignor must track the consignment in real time by a satellite positioning system.

7.4.6 Transportation by Road

Transportation by road may be used for consignments of Material under the following conditions:

a) As a minimum two individuals must escort classified consignments. While being transported the Classified Material must, at all times, be under the security oversight and control of at least one of the carrier company's personnel;

b) For the transportation of SECRET Material a minimum of two individuals (usually the driver and co-driver) must have been granted a security clearance to at least the level of SECRET. For the transportation of CONFIDENTIAL, as a minimum, one of the individuals (either the driver or the co-driver) must have been granted a security clearance to at least the level of CONFIDENTIAL;

c) The Classified Material must be afforded appropriate security protection and must be secured in vehicles or containers by a lock or padlock of a type approved by the NSA/DSA of the consignor. Closed van or cars that may be sealed should be used since they offer maximum security;

d) Exceptionally, if the classified consignment cannot be appropriately secured in a closed vehicle, the consignment must be encased or sheathed so as to protect the classified aspects and prevent unauthorised persons from gaining access. Containers must bear no visible indication of their contents.

e) During brief stops at least one security cleared individual must at all times remain with the vehicle;

f) In cases where overnight stops are necessary, arrangements must be made to use secure storage provided by government or Facility Security Cleared establishments having the appropriately cleared personnel and the capabilities to handle the classified consignment. In the event that such arrangements cannot be made or an emergency situation arises due to accident or breakdown of the vehicle, the cleared driver and/or co-driver, is responsible for keeping the consignment under constant protection during the period.

7.4.7 Transportation by Rail

Transportation by rail may be used for consignments of Material only in the following conditions:

a) Where necessary passenger accommodations should be made available for security guard personnel;

b) during stops, the security escort must remain with the consignment.

Depending on the volume of the consignment, priority should be given to rail cars or containers that can be closed and sealed, giving maximum security.

7.4.8 Transportation by Sea

The following minimum standards are to be applied when consignments of Material classified CONFIDENTIAL or SECRET are sent by sea:

a) consignments should be carried in ships sailing under the flag of an OCCAR Member State or a Programme Participating State. Ships sailing under the flag of a Non-OCCAR or Non-Programme Participating State, which represents a special security risk must not be used unless all of the NSAs/DSAs of the Programme Participating States all agree. The masters of all ships used to carry consignments of Material classified CONFIDENTIAL or SECRET should be nationals of OCCAR Member State or of a Programme Participating State and must hold an appropriate PSC, otherwise an appropriately cleared escort must accompany the consignment;

b) Material must be stowed in locked stowage space approved by the NSA/DSA of the consignor; when this is not available, blocked-off stowage may be approved. Blocked-off stowage is stowage in the hold of a ship where the Material is covered and surrounded by other cargo consigned to the same destination in such a way that, in the opinion of the designated security officer, access to the Material is physically impracticable. Where it is impracticable to carry a consignment in the hold, it may be carried as deck cargo, provided it is in a secure container and packaged so it is not evident that it contains classified Material. In all cases, the consignment must be under security control;

c) stops at maritime countries presenting special security risks must be assessed by the NSAs/DSAs concerned in the light of the political environment, when they receive the transportation plan drawn up by the consignor and the consignee. Unless the ship is in an emergency situation, it must not enter the territorial waters of any of these countries;

d) in all cases, loading and unloading must be under security control and 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. Where this is unavoidable, sufficient security guards must be provided to keep the consignment under adequate supervision, unless it can be stored at a secure facility that is cleared by the consignee's NSA/DSA.

7.4.9 Transportation by Air

Preference must be given to the use of military aircraft of an OCCAR Member State or a Programme Participating State to transport Material classified CONFIDENTIAL or SECRET. If utilisation of a military aircraft is not practicable, an approved commercial air carrier may be used. Commercial air carriers from a Non-OCCAR or Non-Programme Participating State, which represents a special security risk, should not be used unless all the NSAs/DSAs of the Programme Participating States agree. The following minimum standards must be observed:

a) every effort must be made to deliver the consignment straight to the aircraft rather than permitting it to be stored in warehouses, etc., at airports and airfields. When a consignment cannot be loaded straight away, it must either be returned, or stored in a NSA/DSA cleared storage facility, or kept under supervision by a sufficient number of security guards to keep the consignment secure;

b) the aircraft must be met on landing and the consignment unloaded, cleared through customs and transported to its final destination under security control. When this is not practicable, the consignment must be kept at the airport, either at a secure facility that is cleared by the consignee's NSA/DSA, or, in case this is not possible, a sufficient number of security guards must be provided to keep the consignment under adequate supervision;

c) intermediate routine stops of short duration may be permitted, provided the consignment remains in the aircraft. However, if the cargo compartment is to be opened, the escort or other appropriately cleared personnel must be available to ensure the protection of the classified Material;

d) in the event the aircraft is delayed at an intermediate stop or has to make an emergency landing, the escort must take all measures considered necessary for the protection of the consignment;

e) countries presenting special security risks must be assessed by the NSAs/DSAs concerned in the light of the political environment, when they receive the transportation plan drawn up by the security officer of the consignor;

f) direct flights must be used wherever possible and except in an emergency, stops at airfields in a Non-OCCAR Member State or a Non-Programme Participating State is not be permitted;

g) a written transportation plan approved by the participating NSAs/DSAs must be in place before the consignment is released to the cargo handling service or to the commercial air carrier.

7.5 Security Escorts for Transports of CONFIDENTIAL or SECRET Information

Individuals acting as security escorts for transports of CONFIDENTIAL or SECRET Material shall hold the nationality of OCCAR or Programme Participating States and shall hold a PSC at the appropriate level. Security escorts may hold the nationality of other countries as agreed in PSIs.

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

It is the responsibility of the consignor and, where applicable, the consignee to instruct security escorts in their duties. Security escorts may, if appropriate, also be given a copy of "Notes for the Courier" and be required to sign a receipt for it.

7.6 Movement of CONFIDENTIAL and SECRET Information to Non-OCCAR Member States or International Organisations

International movement of information classified CONFIDENTIAL or SECRET to a country, which is not a signatory of the OCCAR Convention or to an International Organisation, shall normally be by:

a) Diplomatic Government-to-Government channels;

b) Military Courier;

c) Hand carriage by security cleared Couriers;

d) As freight by security cleared or approved commercial carriers subject to the requirements outlined in para. 7.4 above.

OCCAR and Non-OCCAR Member States or International Organisations may agree in Security Agreements/Arrangements or PSIs on other methods of transmission or transportation.

7.7 Shipment of Crypto Controlled Items

Crypto Controlled Items (CCI) shall be moved internationally and approved in accordance with applicable national security procedures of the dispatching and receiving State. However, the following minimum standards shall be observed:

As a rule crypto equipment shall not be shipped with keys loaded unless authorised by the responsible National Distribution Agency (NDA) for crypto devices when operationally necessary. Where such crypto-equipment and components contain classified key, they shall be protected during their shipment to the same classification level as the key. However, crypto keys shall usually be moved separately from crypto equipment and the movement of crypto keys may be subject to additional security requirements.

The preferred method of international shipment of crypto equipment or CCI is via courier channels established between the NDAs. When such channels cannot be used shipment of crypto equipment or CCI may be carried out by authorised company couriers in accordance with the above requirements for the movement of classified Material.

CCI shall be dispatched in close cooperation with the responsible NDAs in order to allow proper tracking and accounting of incoming and outgoing Crypto/CCI Material on the territory of a Programme Participating State.

Unclassified CCI Material shall be shipped in accordance with applicable requirements of the dispatching country.

Subject to more stringent national rules, which may be applicable in an OCCAR Member State or a Programme Participating State on movement of classified CCI the following minimum requirements shall be applied for the international movement of CCI:

Prior to shipping CCI, which is classified at the level of RESTRICTED or above a special Transportation Plan for the movement of CCI shall be prepared describing approved movement routes, identifying national NDAs, names of authorised courier companies as well as details of approved consignor or supplier facilities and consignee facilities or authorised recipients of Crypto/ CCI Material (e.g. local crypto custodians or COMSEC officers);

The Transportation Plan shall be submitted in sufficient time in advance to its responsible national NDA for approval;

The NDA then shall forward the Transportation Plan together with other accompanying shipping Documents as may be required under applicable national rules to the NDA of the country of destination;

Upon approval of the Transportation Plan by the NDA of the country of destination the NDA of the dispatching facility then shall record the outgoing shipment in their national COMSEC account and shall inform the dispatching facility that the shipment can take place;

The dispatching facility then shall send a copy of the approved Transportation Plan to its responsible NSA/DSA and request a Courier Certificate for the shipment of CCI;

The crypto custodian or security official of the dispatching facility shall brief the courier on its specific responsibilities for carrying CCI. NDAs may conduct special briefings of designated couriers carrying Crypto / CCI Material on a regular basis;

The consignment shall be securely packaged in a manner that shall detect tampering and guard against damage in transit; for such purpose CCI may be packed into sealed packages or carrying cases;

The envelope shall bear the name of the custodian of the crypto-equipment at the consignee's facility and the COMSEC account number of the consignor;

The envelope shall also contain a receipt prepared by the crypto custodian of the dispatching facility to be signed by the crypto custodian of the receiving facility which is to be returned to the dispatching crypto custodian via the NDAs involved within four weeks;

The consignment shall be handed out to the designated courier against receipt together with the accompanying paperwork, which is to be placed in a sealed envelope;

The receiving facility shall inform their NDA about the delivery of the CCI in order to be recorded as incoming CCI in the national COMSEC account.

When CCI needs to be hand carried on board of aircrafts specific arrangements or approvals may be required with by air traffic control authorities or flight officers, for instance in case the CCI contains active electronic equipment.

More detailed procedures on the international movement of CCI may be contained in PSIs.

8. Visits involving OCCAR CONFIDENTIAL or OCCAR SECRET Information

8.1 General

Subject to the provisions in para. 6 the arrangements described in this para. of the Security Regulations apply to military and civilian representatives of OCCAR Member States, OCCAR Contractors and Sub-Contractors and personnel from OCCAR-EA Establishments who need to undertake visits to a Government department or establishment of another OCCAR Member State, the facilities of a Contractor or Sub-Contractor of another OCCAR Member State or an OCCAR-EA Establishment and require or may have access to information classified CONFIDENTIAL or SECRET – hereafter referred to as Classified Visits.

The procedures for visits by representatives from non-OCCAR Members States shall be described in PSIs.

8.2 Security Requirements for Visits

Such Classified Visits are subject to the following conditions:

a) The visit has an official purpose related to OCCAR activities;

b) The visitor has a Need-to-Know the information related to the specific OCCAR activity;

c) The visitor(s) holds an appropriate PSC;

d) In case of visits from industrial facilities or consultants, the sending facility holds a Facility Security Clearance, if appropriate.

A formal Request for Visit through Government channels and approval by the Security Authority of the host Nation shall not be required.

8.3 Visit Requests

Prior to arrival at a facility identified under para. 8.1 above, information about the visitor shall be provided directly to the receiving facility by the Security Officer of the sending facility using Form OMP 11-5 (OCCAR Visit Request).

To confirm identity the visitor must be in possession of an ID card or passport for presentation to the security authorities at the receiving facility.

Such requests shall be issued for OCCAR-EA Staff Members by the OCCAR-EA Security Officer, for Government representatives of OCCAR Member States by the responsible departmental security officials and for employees of industrial facilities by the company security officers.

8.4 Security Responsibilities

It is the responsibility of the receiving establishments' security official to check with its NSA/DSA, and in case of OCCAR-EA with the responsible OCCAR-EA security organisation, that the sending facility is in possession of the appropriate Facility Security Clearance, and that requirements for access to Classified Information outlined in para. 5, e.g. the consultation process, have been met.

Both the sending and receiving establishment must agree that there is a Need-to-Know for the visitors.

The receiving establishment shall also ensure that records are kept of all visitors, including:

a) Their name;

b) The organisation they represent;

c) Date of expiry of the Certificate of Security Clearance;

d) The date(s) of the visit(s), and

e) The name(s) of the person(s) visited.

Such records are to be retained for a period no less than two years or in accordance with national requirements.

NSA's/DSA's of OCCAR Member States or other States participating in an OCCAR Programme may require prior notification from their Government establishments or industrial facilities to be visited for visits of more than 21 days duration and grant approval, if deemed necessary.

However, should a security problem arise, the NSA/DSA of the State hosting the visit shall consult with OCCAR-EA or the NSA/DSA of the visitor.

9. Security of Communication and Information Systems

9.1 General Requirement

The provisions outlined in this para. define the regulations for OCCAR CIS Security. Their purpose is to establish an acceptable level of confidence across all OCCAR stakeholders that OCCAR Classified Information handled in electronic form is afforded protection from deliberate or accidental compromise, without inhibiting its use, specifically concerning:

- **Loss of Confidentiality** – unauthorised disclosure or compromise of information to unauthorised individuals;
- **Loss of Integrity** – corruption or unauthorised alteration of information;
- **Loss of Availability** – untimely access to information by authorised staff.

9.2 Scope

Any communication and/or computer hardware that intends to store, forward, or process OCCAR Classified Information (hereby referred to as OCCAR CIS) shall be subject to compliance against these regulations.

9.3 Minimum Standard

The protection of Classified Information within CIS relies upon the balanced and proportionate application of measures designed to control and reduce the likelihood of information compromise.

These regulations draw upon the variation and diversity of CIS Security measures already established within national CIS Security Policies, in order to develop a common minimum standard for Security of CIS handling OCCAR Classified Information across the OCCAR community.

9.4 Principles

OCCAR CIS Security is established by the following core principles:

a) Releasability of Information;

b) CIS Accreditation;

c) Proportionality;

d) Documented Procedures;

e) Through-Life Management;

f) Acknowledged Equivalency.

9.4.1 Releasability of Information

The guiding principle of security within OCCAR is the implementation of a "Need to Know" culture, as outlined in the OCCAR Security Agreement and clarified further in para. 10. In this respect:

All CIS shall ensure that information is only released to entities or individuals who have a legitimate and authorised need to access the information for the purposes of their ongoing ability to perform their duties in support of an OCCAR programme.

9.4.2 Accreditation

To ensure control over the release of information (confidentiality), and to safeguard the integrity and availability of that information over time, a governance process shall be established to manage the application and validation of the minimum set of CIS Security controls:

All CIS intending to store, forward, or process OCCAR Classified Information shall obtain prior approval to operate. This shall be achieved by successfully undertaking an accreditation process overseen in accordance with para. 9.5.1. CIS shall demonstrate compliance with these regulations specifically the minimum technical requirements as outlined in Annex OMP 11-E (for OCCAR CONFIDENTIAL and above) and Annex OMP 11-F (for OCCAR RESTRICTED).

9.4.3 Proportionality

To avoid the application of inappropriate or unnecessary security controls or processes in OCCAR CIS, any CIS Security governance process shall accommodate flexibility in requirements based on the perceived threats a CIS may be exposed to:

The level of scrutiny to which a CIS should be expected to undergo to achieve accreditation (principally the quantity and type of evidence to be generated and reviewed) shall vary proportionately with the type of CIS and the threats it will be exposed to.

9.4.4 Through-life Management

To ensure OCCAR CIS remain fit for purpose after initial accreditation and throughout their operational life, any established governance process must consider the through-life aspects of managing and maintaining CIS against a backdrop of ever-evolving cyber threats and challenges:

CIS Security Accreditation of a CIS shall have a limited duration, after which the CIS shall be re-accredited. The duration of accreditation shall be representative of the type of CIS, its intended service life and the types of evolving threats the CIS will be exposed to.

Additionally, any major changes to the CIS operating environment, concept of use or configuration; and any event impacting upon the security of the CIS, shall trigger re-evaluation of the CIS' security documentation so that the Security Accreditation Authority (SAA) may decide an appropriate course of action. This may include the

implementation of further CIS Security controls, or the application of conditional limitations on the CIS' operational capability.

9.4.5 Documented Process

To facilitate effective and proportionate management of CIS Security throughout a CIS' operational life, accreditation shall be granted based upon appropriately verified Security Documentation:

CIS Security accreditation shall be supported by a proportionate level of documented, configuration-controlled evidence describing an accurate representation of the implemented CIS design and operational use.

9.4.6 Equivalency of Accreditation

CIS accredited to handle national Classified Information by OCCAR Member States shall also be authorised to handle OCCAR Classified Information of an equivalent classification (as defined in Annex OMP 11-B Table of Equivalent Security Classifications) provided that the requirements are not less stringent than OMP 11.

9.5 Roles and Responsibilities

CIS Security is a complex and highly technical subject that requires the identification and staffing of appropriately trained and skilled personnel resources. In principle, there are three key roles involved with approval of CIS:

- The Security Accreditation Authority (SAA) – ultimately responsible for overseeing the process and deciding on the acceptability of a solution;
- The Planning and Implementation Authority (PIA) – responsible for the development of a secure CIS design, and putting it into place in consultation with the SAA;
- The System Operating Authority (SOA) – the entity that will become responsible for the system once it becomes operational.

Each of these roles (or equivalents) shall be established for all OCCAR CIS. Although the authorities and entities responsible shall vary depending on the context of a CIS, they shall have the following responsibilities and decision-making capabilities:

9.5.1 Security Accreditation Authority

The SAA is a technically competent authority responsible for:

a) Providing advice on CIS Security issues;

b) Defining which CIS Security accreditation process shall be used (for instance, National CIS Security Policies) and outlining the conditions for the accreditation of a CIS under their authority;

c) Reviewing and approving the CIS Security documentation;

d) Reviewing additional documentation such as Concepts of Operation, system/product certification reports and security feature user guides;

e) Providing a statement of compliance with the established security accreditation process for the CIS, stating the conditions under which the system may operate, and those against which re-accreditation is required;

f) Checking the implementation of security arrangements for the CIS under its responsibility, for instance through periodic security inspections in accordance with the security accreditation process;

g) Liaising with PIAs and SOAs in respect to through-life security management;

h) Providing direction for the investigation of security breaches, suspected breaches of the security arrangements in place;

i) Advising on the security risk and associated implications of proposed changes to a CIS;

j) Liaising with other security accreditation authorities in respect to interconnected CIS.

CIS intending to store, forward or process OCCAR Classified Information can be authorised for use by various SAAs within the OCCAR community; in particular OCCAR Member States, Programme Participating States and the OCCAR Executive Administration.

The type of approval, and thus the Accreditation Authority responsible for approving OCCAR CIS shall depend upon the way in which a CIS will operate or interact with other CIS.

- CIS that are developed for the sole use of a single OCCAR entity, or are designed to be hosted entirely within the scope of responsibility of a single OCCAR entity, shall undergo approval against an OMP 11-equivalent CIS Security accreditation or approval process overseen by that OCCAR entity's security accreditation or approval authority.

- Where national laws and regulations of OCCAR Member States and Programme Participating States allow, the SAA activities of CIS handling OCCAR RESTRICTED information may be delegated to Contractors[1]. In such circumstances, Annex OMP 11-C (The Handling of OCCAR Restricted Information by Contractors) and Annex OMP 11-F (CIS Security requirements for OCCAR Restricted Information) shall be provided by the Contracting Authority to the Contractor. Nevertheless, where this delegation is exercised, the relevant NSAs/DSAs shall retain overall responsibility for the protection of OCCAR RESTRICTED information handled by the Contractor, and the Contract shall include provisions permitting the Contracting Authority and relevant NSA/DSA according to national laws and regulations, the right to inspect the security measures taken by the Contractors. In addition, the Contractor shall provide the Contracting Authority and, where appropriate, the NSA/DSAs with a statement of compliance certifying that the CIS handling OCCAR RESTRICTED information has been accredited in compliance with these regulations. The NSA/DSA is the acknowledged

[1] This is exercised by Belgium, France, Germany, Spain, and UK.

authority having responsibility for certifying at international level that the CIS handling OCCAR RESTRICTED information has been accredited.

- CIS that are developed specifically for use by more than one OCCAR entity in support of an OCCAR Programme shall undergo a joint accreditation process overseen by an SAA composed of NSA/DSA representatives from all OCCAR entities involved;

- Interconnections between CIS that are already approved to store OCCAR (or, in accordance with para. 9.4.6, equivalent National) Classified Information, shall undergo a joint accreditation process overseen by an SAA composed of NSA/DSA representatives from all OCCAR entities involved in the interconnection.

In this context "OCCAR entity" refers to a single OCCAR Member State, Programme Participating State or the OCCAR Executive Authority.

9.5.2 Planning and Implementation Authority

The PIA is the technically competent entity responsible for developing and implementing the design of the CIS in conjunction with SOAs, project staffs and the SAA. In particular they shall:

a) providing advice and guidance on the technical and implementation aspects of CIS Security to the SAA;

b) advise the CIS operating authority of CIS Security technical and implementation aspects of proposed changes to the CIS configuration, a change in its operational requirement or a change in the classification level of information being stored, forwarded or processed by the CIS;

c) provide the CIS Security design requirements (for example, network and operating system security requirements, boundary protection component requirements, malicious software prevention requirements, and security management tools requirements, including intrusion detection / prevention systems) for the CIS;

d) developing and maintaining detailed technical design documentation clearly specifying the configuration of system components, in particular those relating to security, or providing security enforcing functions;

e) developing and maintaining the Security Documentation and any additional Security-related documentation required by the SAA.

9.5.3 System Operating Authority

The SOA is the organisation responsible for taking decisions related to the System's Purpose, configuration and ultimately its day-to-day operation. This may be the same entity as the PIA.

9.6 Accreditation

The term "Accreditation" is used to define the management process through which CIS Security governance is achieved; its aim is to generate appropriate Security Documentation, often referred to as an Accreditation Document Set (ADS), upon which a decision to approve or reject the use of a CIS may be made.

Accreditation consists of 4 stages: Evaluation, Verification, Testing and Validation.

9.6.1 Evaluation

The first stage of CIS Security accreditation involves formal review of the Security Documentation and any other supporting Security or technical documentation by the SAA in order to identify unacceptable concerns regarding the design or operational posture of the CIS.

As a paper-based exercise, any issues may be addressed through updates to the design prior to installation with minimal impact to project time, cost or performance. Once the SAA endorses the evaluated design and security documentation, the PIA may embark upon the installation process.

9.6.2 Verification

Once a CIS is installed, it is necessary to verify that it has been setup and configured in accordance with the evaluated design and security documentation.

The aim of verification is to scrutinise the functionality of specific security devices or security enforcing functions identified by the SAA as being important to the overall security of the CIS by subjecting them to controlled security testing in accordance with a Security Test and Verification (ST&V) plan.

Where these tests are successful, the SAA can gain confidence that the installed system is an accurate implementation of the intended design, verifying that an accurate configuration baseline has been established upon which configuration management can begin.

9.6.3 Testing

An essential aspect of CIS Security is the availability of the services and/or capabilities that CIS intend to provide. Given that technical security measures introduce inherent complexity to a system (especially when compared with an open development environment) it is necessary to check that the system can still perform its functions in its secured state.

The CIS shall therefore be subject to robust and comprehensive functional testing in order to validate that the system can operate in accordance with its Concept of Use in a secure way.

9.6.4 Validation

Once the CIS has been successfully evaluated, verified and tested, the SAA has the necessary information to validate the claims made by the PIA that the system is secure and authorize the system to operate with either:

a) **Full accreditation** – This is the ultimate aim of all OCCAR CIS, as it demonstrates that the CIS Security measures implemented within the CIS are sufficient to allow unconditional use of the system within the operational environment as defined within the associated Security Documentation. This approval shall last for a specified timeframe as agreed by the SAA; or

b) **Conditional accreditation** – In some circumstances, the SAA may allow a CIS to operate despite observing security risks. In these cases, special conditions shall be applied to the authorisation, limiting its operational use or technical capabilities in order to minimise the risk of compromise or exploitation.

In practice this is likely to apply to existing fully-approved systems that are unexpectedly exposed to new vulnerabilities or threats, or new systems whose CIS Security measures are not currently fit for purpose but whose capabilities are required for operational reasons.

The duration of conditional accreditation shall be much shorter than full accreditation, as agreed by the SAA.

Confirmation of accreditation is facilitated by the issue of a document stating the level of compliance with the SAA's nominated OMP 11-compliant CIS Security accreditation process, including any conditions or limitations on its use as a result of conditional accreditation.

9.7 Documentation

The evidence required to support CIS Security accreditation shall be provided in the Security Documentation. This will include the following types of Documents, or national equivalents.

9.7.1 Security Accreditation Strategy

A Security Accreditation Strategy (SAS) shall be developed by each SAA, establishing a conceptual accreditation process for a particular CIS. The purpose of the SAS is to allow customisation of security requirements in accordance with National or international standards or policies, and the appetites of specific SAAs.

Depending on the type of accreditation processes being followed, it may be acceptable to develop a standardised SAS that outlines a generic accreditation strategy that can be followed by multiple CIS. For example, existing national CIS Security policies may already define a SAS for all CIS operating at OCCAR RESTRICTED within the responsibility of a single SAA.

9.7.2 Security Management Plan

A Security Management Plan (SMP) shall be developed by the PIA to demonstrate how they intend to comply with the accreditation process defined in the Security Accreditation Strategy.

To ensure CIS Security issues are identified and resolved as early as possible, the SMP (or national equivalent) shall be prepared for endorsement by SAAs as early as possible. As a minimum, the SMP will include:

a) The size and capabilities of the CIS;

b) The classification and volume of information stored, forwarded or processed by the CIS;

c) The security clearance levels of the CIS users;

d) The scope of any sites or environments in which the CIS may operate;

e) The conditions in which the CIS intends to operate;

f) The application of the need-to-know principle and the requirements for information sharing;

g) Any planned interconnections with details of external CIS;

h) The security risks associated with the information and supporting services and resources, and any measures necessary to mitigate them;

i) The security risk assessment processes that will be applied to ensure security measures are appropriate, including any required security evaluation or certification;

j) The schedule, against which CIS Security deliverables shall be provided, evaluated, verified and validated.

The SMP (or national equivalent) shall be updated as required by the SAA.

9.7.3 Security Requirement Statements

For certain Systems handling Classified Information, various Security Requirement Statements (SRS) may be produced detailing how the system and/or interconnections shall protect the information they intend to store, forward, or process.

All SRS shall be developed in coordination with the SAA as early as possible in the design phase. The following SRS may be applicable to OCCAR CIS:

a) Community SRS (CSRS) – for interconnected or joint accreditations, it is necessary to define and agree certain requirements across the community of stakeholders involved in the project. This establishes clearly defined boundaries of responsibilities and associated expectations over information exchanges.

b) System SRS (SSRS) – for local area networks or stand-alone systems it is essential for design authorities to clarify and agree with their SAAs what requirements need to be met. The SSRS is a living Document that evolves alongside a CIS design, documenting key risk factors and associated Security Enforcing Function requirements.

c) System Interconnection SRS (SISRS) – specific to individual connections, SISRS allow all stakeholders to clearly define Information Exchange Requirements and the measures necessary to enforce them (and associated protection mechanisms) to maximise interoperability while establishing clear communication mechanisms to deal with potential security incidents.

As a minimum, the SRS shall describe the following aspects of the CIS Security requirements:

a) Any specific risks for the systems or interconnections;

b) The operational environments of the systems and interconnections;

c) The level and frequency of Classified Information to be processed, stored or transmitted;

d) The nature of Classified Information (e.g. optical or acoustical signals, information in writing);

e) The hardware and software configuration and features of the systems and of supporting devices (system architecture);

f) Software and hardware security features;

g) TEMPEST and/ or COMSEC measures to be applied (including encryption systems used);

h) Personnel, physical and administrative security measures;

i) Security operating procedures or user instructions.

SRS may be supported by, or based upon the baseline technical requirements outlined in Annex OMP 11-E and Annex OMP 11-F.

9.7.4 Security Test & Verification Plan & Reporting

A ST&V Plan is a description of the security testing to be performed in order to verify the CIS Security measures defined in the Security Documentation have been effectively deployed within the implemented design.

For each security-relevant or security-enforcing function, as determined by the SAA in the Security Documentation, the following shall be identified:

a) the objective of the security test;

b) an outline description of the security test;

c) a description of the execution of the security test; and

d) the results of the security test.

The security test and verification requirements necessary in any given circumstance is determined by the SAA in conjunction with the CIS planning and implementation authority(s), operating authority(s) and project staffs. The SAA shall be responsible for approving the ST&V plan and the results of the security testing as part of the security accreditation process.

9.7.5 Baseline Compliance Checklist

These regulations allow for a simplified accreditation process for isolated systems called a Baseline Compliance Checklist (BCC). Combined with robust Security Operating Procedures (SecOPs) and a Statement of Compliance, the baseline checklist can be used as the minimum for accreditation of low-risk, stand-alone OCCAR CIS.

The CIS Security Baseline Control Sets in Annex OMP 11-E and Annex OMP 11-F (for OCCAR CONFIDENTIAL and OCCAR RESTRICTED respectively) have a column that can be used as a checklist of CIS Security compliance. By ensuring the measures defined within the SecOPs meet the requirements documented in the SRS for a given system, an SAA may use the baseline control set as a checklist for authorising the storing, forwarding, or processing of OCCAR information within low-risk CIS.

Note that the controls outlined within these annexes may be individually waivered (so long as justification is given as to why the control is not necessary for a given CIS) or supplemented with additional requirements by an appropriately authorised SAA as documented in the relevant Security Requirement Specifications. In this regard, the BCC can be used as the basis for developing CIS-specific SRS documentation, or as an isolated checklist to support the development or preparation of other Documents such as SRS.

9.7.6 Security Operating Procedures

The SecOPs is the key Document in the Security Documentation of a CIS. Their aim is to describe in detail, the specific implementation of the various CIS Security controls as mandated within the various SRS. In particular, the SecOPs will outline the measures used to manage:

a) administration and organisation of security;

b) personnel security, physical security, security of information;

c) technical CIS Security;

d) emergency and contingency planning; and

e) configuration management.

The level of detail and complexity of a CIS' SecOPs shall vary depending on the complexity of the CIS being developed. Ultimately, the SecOPs should explain to the SAA exactly how the technical requirements outlined in the baseline checklist have been fulfilled by the CIS design in order for it to be evaluated, verified and validated as part of the accreditation process.

9.7.7 Applicability

The SAA of a CIS has final decision over what documentation is required to support accreditation, and as such should be involved as soon as possible in the developing and planning process of OCCAR CIS.

These regulations recommend proportional constraint when specifying Security Documentation requirements. Ideally, the type of documentation required to support accreditation of OCCAR CIS should vary in quantity and complexity depending on the type of system being accredited. By example, accreditation processes should differentiate between high-risk interconnected CIS and those CIS that intend to operate in isolation:

- Isolated CIS are composed of a single workstation or Local Area Network with dedicated peripherals (Printers, scanners, or other input devices) that are not (and will never be) connected to other networks.

- Interconnected CIS are composed of one or more systems that are intended to be connected with other systems via means of networking technologies.

The suggested proportionality of required documented evidence for such diverse CIS is summarised in Table 1.

	Classification:	OCCAR RESTRICTED	OCCAR CONFIDENTIAL or above

	Type of CIS:	Isolated	Interconnected	Isolated	Interconnected
Documentation	Security Accreditation Strategy		✓	✓	✓
	Security Management Plan		✓	✓	✓
	CSRS		✓		✓
	SSRS		✓	✓	✓
	SISRS		✓		✓
	ST&V Plan & Report		✓	*	✓
	Baseline Compliance Checklist	✓		*	
	SecOPs	✓	✓	✓	✓

Table 1 - Applicability of approval processes and required documentation.
*** As agreed by SAA.**

10. Release of Classified Information

10.1 General Requirement

Classified Information shall be released only with the prior consent of the Originator.

10.2 Release of Classified Information to OCCAR Member States not Participating in an OCCAR Programme or to Contractors located in such States

10.2.1 Release of Classified Programme Background Information

Classified Programme Background Information shall only be released to OCCAR Member States not participating in the Programme or to Contractors located in such states with the prior written consent of the originating State or International Organisation.

10.2.2 Release of OCCAR Classified Programme Foreground Information

Classified Programme Foreground Information shall only be released to OCCAR Member States not participating in the Programme or to Contractors located in such states with the prior written consent of all countries participating in the Programme.

10.3 Release of OCCAR Classified Information to Non-OCCAR Member States, or to Contractors located in such States, or to International Organisations

The release of OCCAR Classified Information to

a) a Government establishment of a Non-OCCAR Member State;

b) a Contractor or Sub-Contractor located on the territory of a Non-OCCAR Member State, or

c) an International Organisation

shall require:

a) the prior release approval by the Originator or the Programme Participating States, respectively and;

b) a Security Agreement or Arrangement (para. 10.4) and, where applicable, a Security Assurance (para. 10.5).

10.4 Security Agreements or Arrangements

Before any OCCAR Classified Information may be released to Non-OCCAR Member States or International Organisations OCCAR shall conclude Security Agreements or Arrangements with such States or International Organisations.

Such Security Agreements or Arrangements shall cover the protection of OCCAR Classified Information and the protection of Classified Information of the respective Non-OCCAR Member States or International Organisations exchanged between the Parties/Participants or released to Contractors located in the Non-OCCAR Member State Party/Participant.

Security Agreements or Arrangements between OCCAR and International Organisations shall ensure by using access and distribution limitations that OCCAR Classified Information may only be distributed to the Member States of the International Organisation which have a need-to-know.

Security Agreements or Arrangements may be general or limited in scope to an OCCAR Programme.

Provisions of such Security Agreement or Arrangement, as a Security Statement, may be part of any other agreement or arrangement (i.e. Programme Decision) concluded between OCCAR and Non-OCCAR Member States or International Organisations.

Any negotiation of Security Agreements or Arrangements shall be subject to the prior approval of the BoS.

The preference is for legally binding Security Agreements or Arrangements. Non-legally binding Security Agreements or Arrangements require explicit SC endorsement and BoS approval.

OCCAR-EA shall negotiate any such Security Agreements or Arrangements with Non-OCCAR Member States or International Organisations subject to consultation with and endorsement by the OCCAR SC and final approval of the BoS.

The protection of national Classified Information of OCCAR Member States by Non-OCCAR Member States or International Organisations and the protection of Classified Information of Non-OCCAR Member States or International Organisation by OCCAR Member States is subject to bilateral Security Agreements or Arrangements between OCCAR Member States and Non-OCCAR Member States or International Organisations.

10.5 Security Assurances

In the absence of a Security Agreement or Arrangement between OCCAR and a Non-OCCAR Member State, OCCAR Programme Foreground Classified Information may exceptionally and in the circumstances described below be released to that State or to a Contractor located in such a State under sponsorship by an OCCAR Member State Participating in the specific OCCAR Programme subject to the following requirements:

a) A bi-lateral Security Agreement or Arrangement is in place between the sponsoring OCCAR Member State Participating in the Programme and the respective non-OCCAR Member State;

b) The sponsoring OCCAR Member State Participating in the OCCAR Programme obtains with the approval of the BoS and OCCAR Programme Participating States a Security Assurance signed by an appropriately authorised official of the receiving Non-OCCAR Member State regarding the protection of OCCAR Programme Classified Information. The Security Assurance shall make reference to the bi-lateral Security Agreement or Arrangement, identify the authorities that signed it together with the date of expiry if applicable. The Security Assurance shall also identify the OCCAR security classifications and the equivalent security classifications of the Non-OCCAR Member State and of the sponsoring OCCAR Member State Participating in the OCCAR Programme as identified in the bi-lateral Security Agreement or Arrangement.

Only OCCAR Classified Information up to and including OCCAR CONFIDENTIAL may normally be released through Security Assurances.

Where there is a requirement to release OCCAR SECRET information through a Security Assurance, the sponsoring OCCAR Member State Participating in the Programme shall provide the necessary assurance that the appropriate security system is in place for the protection of such released information.

If the recipient is a Contractor and if the sponsoring OCCAR Member State Participating in the OCCAR Programme does not have the jurisdiction over the Contracting Authority, the NSA/DSA with jurisdiction over the Contracting Authority must be provided with the Security Assurance and a copy of the Security Agreement or Arrangement. The written consent of the Nation with jurisdiction over the Contracting Authority is required otherwise the Contract shall not be placed.

The signed Security Assurance shall be provided to OCCAR-EA and the other OCCAR Programme Participating States.

The BoS's and OCCAR Programme Participation States' approval given prior to the use of a Security Assurance instead of the negotiation of a Security Agreement or Arrangement between OCCAR and the relevant Non-OCCAR Member State is acceptable provided that the release of OCCAR Classified Information is related only to:

a) The export (including pre-export marketing) of defence equipment procured within one OCCAR Programme and provided the Programme Participating States agree with the export;

b) The services or supplies provided by a Sub-Contractor within one OCCAR Programme and provided such services and supplies are limited in terms of scope, and duration.

c) The urgent need to release OCCAR Classified Information for collaborative or operational reasons to governmental organisations in non-OCCAR Member States.

10.6 Release Procedures

Unless stated otherwise in OCCAR PSIs any release of Classified Information shall be as described hereinafter.

10.6.1 Release of Classified Programme Background Information

Requests for release of Classified Programme Background Information shall be submitted directly to the originating State's NSA/DSA or any other competent national authority, or the security body of the International Organisation.

Contractors or Sub-Contractors shall submit such requests via their respective NSA/DSA or any other competent national authority.

10.6.2 Release of Classified Programme Foreground Information

Requests for release of Classified Programme Foreground Information by Contractors or Sub-Contractors shall be submitted to the respective OCCAR-EA Programme Division, which shall forward the request to the Programme Committee (PC) for consideration and approval.

Sub-Contractors shall submit such requests to OCCAR-EA via their Contracting Entity.

National Government establishments shall submit their requests directly to the respective PC.

Prior to taking a decision on the release of OCCAR Classified Information the national PC representatives shall review, in coordination with their competent national authorities involved, the release requests in accordance with relevant national rules.

If a decision on such release cannot be reached in the PC the issue shall be referred to the Programme Board for decision.

11. Industrial Security & Contracting

11.1 General

For each OCCAR Programme OCCAR-EA shall, in co-operation with the Programme Participating States, prepare a PSI and a SCG.

Where the classified activities under a Programme are of limited nature (e.g. preparation of studies during initial phase of a Programme) the specific security aspects of a Programme may be defined in SALs.

11.2 General Responsibilities

The Programme Participating States' relevant security authorities shall be responsible for the implementation of the PSI within their Government establishments and Contractors involved in the Programme pursuant to the OCCAR Security Regulations.

Prior to the release of information classified CONFIDENTIAL or SECRET to a Contractor, prospective Contractor, or Sub-Contractor, the relevant OCCAR Member State or other Programme Participating State, as appropriate, in accordance with its national procedures shall:

a) Ensure that such Contractor(s), prospective Contractor(s), or Sub-Contractor(s) and their facility(ies) have the capability to protect the information adequately;

b) Grant PSCs to all personnel whose duties require access to Classified Information in compliance with the provisions of para. 4;

c) Ensure that access to the Classified Information is limited to those persons who have a Need-to Know for purposes of performance on the OCCAR activity;

d) Upon request of OCCAR-EA or any OCCAR Member State or other State participating in an OCCAR Programme grant a FSC to enable a company to negotiate or perform an OCCAR Classified Contract, Sub-Contract or call for tenders;

e) Provide, upon request, to OCCAR-EA, an OCCAR Member State or any other State participating in an OCCAR Programme a PSC for the individuals for whom it has security responsibilities to enable them to perform on an OCCAR Classified Contract, which may also include international visits;

f) Take action with regard to the specific arrangements to be carried out in matters of transportation in accordance with para. 7.4;

g) Ensure that, for any Contractor facility where Classified Information is handled, suitable persons are appointed to effectively exercise the responsibilities regarding the protection of Classified Information. These individuals shall be responsible for limiting access to the Classified Information provided or generated under a Contract to such persons holding a security clearance, when necessary, and who have been properly approved for access, and who have a Need-to-Know.

OCCAR Member States or any other State participating in an OCCAR Programme shall investigate all cases in which it is known or where there are grounds for suspecting that Classified Information provided or generated pursuant to an OCCAR Contract being undertaken in its territory has been lost or disclosed to unauthorised persons. OCCAR Member States and States participating in an OCCAR Programme shall comply with the investigative requirements in para. 12 of this Document.

11.3 Contracts and Sub-Contracts Involving CONFIDENTIAL or SECRET Information

All Contractors and Sub-Contractors providing services, deliveries or supplies in connection with an OCCAR Programme, which require access, generation or retention of Programme Information classified OCCAR CONFIDENTIAL or above shall hold a FSC at the appropriate level issued by the responsible NSA/DSA of the country in which the Contractor or Sub-Contractor is located.

OCCAR-EA shall be the Contracting Authority for prime Contracts let in connection with an OCCAR Programme.

Sub-Contracts shall be let by the responsible Contracting Entity of a Contractor already engaged in the performance of an OCCAR Contract or Sub-Contract.

11.4 Application of Security Classifications by Contractors

The following general principles shall be observed in connection with the security classification requirements of OCCAR Classified Contracts:

a) The allocation of classification levels is the responsibility of the entity creating the Classified Information following the guidance provided in applicable SCGs or Security Aspects Letters;

b) A compilation of information at a given classification level may justify a classification at a higher level; the items constituting a compilation shall be identified in the SCG, if appropriate;

c) Provision for Downgrading or Declassification should be made as early as possible, preferable when creating the information;

d) Changes to the classification level should be made only with the permission of the Originator.

In cases where no or no sufficient guidance on security classification is given for Contract deliverables for instance in connection with definition, design or development activities, the Contractor shall propose suitable classifications to the Contracting Authority, which shall arrange for coordination and approval by the Programme Participating States' competent national authorities.

11.5 Pre-contractual Activities / Contract Negotiations / Invitations to Tender

Before entering into negotiations for a Contract or Sub-Contract involving the release of Programme Information classified OCCAR CONFIDENTIAL or OCCAR SECRET the Contracting Entity shall via its responsible NSA/DSA submit a request to the NSA/DSA of the country where the potential Sub-Contractor is located in order to obtain confirmation that the potential Contractors hold a FSC at the required level. In case the potential Sub-Contractor does not hold the required FSC, the responsible NSA/DSA shall be requested to initiate the clearance procedure.

The request for a FSC shall provide sufficient information regarding the classification level and the nature of services or supplies requiring access or potential access to Classified Information in order to allow the responsible NSA/DSA to make the necessary security arrangements at the Sub-Contractor's facilities.

For exchange of information relating to a FSC the relevant OMP 11 guidance form shall be used.

Where a Contract does not require the potential Contractor to hold Classified Information at the level of OCCAR CONFIDENTIAL or OCCAR SECRET at the tender stage potential Contractors not holding an FSC may be invited to tender for the Contract but such Contractors must be advised in the tender documentation that the company/facility shall be required to be granted an FSC should it be selected to undertake the Contract and that Contract award is subject to the FSC being granted.

Should a Contractor facility without an FSC be selected, the Contracting Entity must request the relevant NSA/DSA to initiate action to grant the Contractor facility an FSC to at least the classification level of the security aspects of the Contract to be undertaken. The Contract must not be awarded until the NSA/DSA has provided an assurance that the Contractor's facility has been granted the FSC. If the FSC cannot be granted, the Contract shall not be awarded.

In case of tenders, all invitations to tender in respect of OCCAR Classified Contracts shall contain a clause requiring a prospective Contractor, who does not submit a bid or who has been notified that his bid was not successful to return all classified Documents or Material, which was provided during the tendering phase to the Contracting Entity.

In invitations to tender for Sub-Contracts the tenderer shall be required to sign an arrangement, which makes the relevant provisions of this Document binding upon the tenderer.

11.6 Contract Security Clauses

Contracts involving access to Classified Programme Information shall contain a clause which makes the relevant provisions of OMP 11 and supplementary security requirements defined in a PSI binding upon the Contractor. In addition, Contract security clauses may outline the security responsibilities of the Contractor and shall oblige the Contractor to respect any instructions given by the Contractor's responsible NSA/DSA regarding the implementation of the OCCAR Security Regulations accordance with applicable national security laws and regulations.

11.7 Sub-Contracting

The Sub-Contracting shall be subject to the restrictions on release of Classified Programme Information as detailed in para. 10.

11.8 Sub-contracting to Contractors in Non-Programme Participating OCCAR Member States

Prior to considering the letting of a Contract to a Sub-Contractor located in non-Programme Participating State, which is an OCCAR Member State and involving the release of OCCAR Classified Information the Contracting Entity shall seek written approval via the contracting chain from OCCAR-EA.

When having obtained written approval for release of OCCAR Classified Information to a Sub-Contractor located in such country a request for a FSC for the Sub-Contractor shall be submitted via the NSA/DSA of the Contracting Entity to the NSA/DSA of the OCCAR Member State where the Sub-Contractor is located.

11.9 Sub-Contracting to Contractors in Non-Programme Participating Non-OCCAR Member States

Prior to considering the letting of a Contract to a Sub-Contractor located in non-Programme Participating State, which is not an OCCAR Member State and involving the release of OCCAR Classified Information the Contracting Entity shall seek written approval via the contracting chain from OCCAR-EA.

When having obtained written approval for release of OCCAR Classified Information to a Sub-Contractor located in such country a request for a FSC for the Sub-Contractor shall be submitted via the NSA/DSA of the Contracting Entity to the NSA/DSA of the country where the Sub-Contractor is located.

Contracts placed with Contractors in a non-Programme Participating and Non-OCCAR Member States shall include a security clause requiring the Contractor to protect OCCAR Classified Information in accordance with the Security Agreement or Arrangement in place between OCCAR and the Contractor's Government or the relevant Security Assurance of the Contractor's Government.

11.10 Notification of Classified Contracts

Contracting Entities shall notify via their respective NSA/DSA the NSA/DSA of the country where the Sub-Contractor is located about any Sub-Contracts involving Classified Information at the level of OCCAR CONFIDENTIAL or above, to include details on the nature of services or supplies or work to be performed by the Sub-

Contractor, the security classification, the nature and volume of Classified Information to be furnished to or to be generated by the Sub-Contractor as well as any other relevant security aspects.

12. Loss or Unauthorised Disclosure OCCAR CONFIDENTIAL or OCCAR SECRET Information

12.1 General Responsibilities

When OCCAR-EA or an OCCAR Member State or any other State participating in an OCCAR Programme discovers or is informed of an incident that has resulted in or where it is reasonable to assume that there has been a loss or unauthorised disclosure of Classified Information immediate action shall be taken in order to:

a) Establish the facts;

b) Assess and minimise the damage done;

c) Prevent a recurrence;

d) Notify the appropriate authorities of the effects of the incident.

12.2 Reports

In case of compromise or loss of classified Programme information, an initial report shall be provided to the relevant NSAs/DSAs and OCCAR-EA within 30 days, to be followed by a detailed report containing the following information:

a) A description of the information involved, including its security classification, reference and copy number, date, entity having created the information, subject and scope;

b) A brief description of the circumstances of the incident, including the date, the time and a statement of whether the provider of the information has been informed.

12.3 Responsibilities for Investigations

Any compromise, loss or other incident where it is reasonable to assume that Classified Information has been compromised or accessed by unauthorised persons shall be investigated by the competent security organisation of the establishment where the incident has occurred. The investigation shall result in a report, which should contain the details as listed in para. 12.2 above.

In case such incident occurs within OCCAR-EA, OCCAR-EA shall report the incident to the NSA's/DSA's of the States participating in the Programme concerned.

12.4 Disciplinary Action

Any individual, who is proven to be responsible for loss or unauthorised disclosure of Classified Information, renders themselves liable to disciplinary action without prejudice to any legal action.

13. Handling of OCCAR RESTRICTED Information

13.1 Applicability

This paragraph describes the requirements for the handling of Documents or Material containing OCCAR RESTRICTED information. Para. 4, 5, 6, 7.1-7.6, 8 and 12 are not applicable.

13.2 Access

Information classified OCCAR RESTRICTED shall only be made accessible to personnel that require such information applying the "Need-to-Know" principle".

All persons having access to OCCAR RESTRICTED Information shall be made aware of their responsibilities for the protection of such information and the consequences of negligence.

Employees who prove to be unsuitable for compliance with the provisions of para. 13 will be excluded from work on OCCAR RESTRICTED Information.

A PSC or a FSC shall not be required for access to OCCAR RESTRICTED Information.

13.3 Release

Release of OCCAR RESTRICTED Information is described in para. 10 and the provisions hereafter.

Except with the written consent given by the Originator the Contractor shall not release RESTRICTED Information to any persons other than employees of the Contractor or to any other Contractor, government or International Organisation not participating or otherwise involved in the OCCAR programme or activity the information relates to.

Requests for the release of such information shall be submitted via the contracting chain to the OCCAR-EA.

13.4 Security Classification, Marking and Declassification

Information shall be classified, marked as OCCAR RESTRICTED and declassified as described in para. 3 and the following paragraph.

The entity creating OCCAR RESTRICTED Information shall ensure that all Documents and copies or reproductions thereof containing such Information will be conspicuously stamped, typed, printed or written in bold and capital letters at the top of the front cover or cover letter and at the top of each page in black or blue colour indicating the overall classification of the Document.

Contractors or Sub-Contractor shall mark any information, which need to be classified OCCAR RESTRICTED, as identified in PSIs or relevant Contract security arrangements.

13.5 Handling and Storage

The Contractor shall not use OCCAR RESTRICTED Information for purposes other than those defined by the Contract.

Documents or Material or computer storage media or interim Material not immediately destroyed and containing OCCAR RESTRICTED Information must not be left unattended or handled in a manner that could result in unauthorised access.

Documents or Material containing OCCAR RESTRICTED Information shall be stored in locked desks, cabinets or similar containers or may be secured in locked rooms/offices provided access to the room is restricted only to persons authorised to have access to the information.

13.6 Reproduction and Destruction

Reproductions of OCCAR RESTRICTED Information shall be produced under conditions that shall prevent unauthorised persons from gaining access. Reproductions of Documents or Material shall be assigned the security classification and markings of the original.

OCCAR RESTRICTED Information, including interim Documents and Material such as working drafts, shorthand notes or spoilt copies shall be destroyed in a manner to ensure that it cannot be easily reconstructed.

To prevent unnecessary accumulation of OCCAR RESTRICTED Information superseded or no longer needed OCCAR RESTRICTED Information shall be destroyed as soon as practicable or returned to the originator. Documents or Material and computer storage media containing OCCAR RESTRICTED Information should be reviewed at regular intervals to determine whether they can be destroyed.

13.7 Movement

Consignments containing OCCAR RESTRICTED Information shall be moved, as a minimum, either by:

a) Ordinary or registered mail;

b) Commercial courier services;

c) Personal carriage by staff members without formal Courier orders.

When moving such OCCAR RESTRICTED consignments, the Documents or Material at least shall be put in a single envelope, package or similar wrapping.

The envelope/package must not bear a classification marking.

In the case of the personal carriage, Documents or Material containing OCCAR RESTRICTED Information shall be kept under the permanent personal custody and must not be left unattended in hotel rooms or vehicles and must not be read or displayed in public.

The movement of CCIs classified OCCAR RESTRICTED is subject to specific requirements involving the competent NDA. The common standards for the shipment of CCI are defined in para. 7.7.

13.8 Communication and Information Systems

The Security of CIS shall follow the procedures as described in para. 9.

13.9 Contracts involving OCCAR RESTRICTED Information

Contracts involving OCCAR RESTRICTED Information shall follow the procedures as described in para. 11.4, 11.6 – 11.9 and as further detailed in this paragraph.

The relevant provisions applicable to Contracts involving OCCAR RESTRICTED Information only are described in Annex OMP 11-C and Annex OMP 11-F.

Contracting Entities of Contracts involving OCCAR RESTRICTED Information only shall be responsible for ensuring compliance of their Sub-Contractors with applicable security provisions for the protection of OCCAR RESTRICTED Information and, if necessary conduct verification visits on Sub-Contractor facilities located in OCCAR Member States or Programme Participating States in coordination with the responsible NSA/DSA.

PSIs or relevant Contract security arrangements shall identify any information, which need to be classified OCCAR RESTRICTED.

All OCCAR RESTRICTED Information generated or received shall be returned to the Contracting Entity upon completion or termination of the Contract, unless the information has been destroyed or authorised for retention. OCCAR RESTRICTED Information approved for retention must be protected in accordance with the provisions of this para. and must not be used for other purposes without the prior written consent of OCCAR.

13.10 Loss or Unauthorised Disclosure

The holder of OCCAR RESTRICTED Information shall investigate all cases in which it is known or there is reason to suspect that such Information has been lost or disclosed to unauthorised persons.

Any such cases must be reported via the relevant NSA/DSA to the OCCAR Programme Participating States' NSAs/DSAs and to OCCAR-EA. Actions may be taken by the competent authorities, as deemed necessary.

13.11 Visit

Visits requiring access to OCCAR RESTRICTED Information only shall be arranged directly between the sending and receiving establishments without formal requirements.

14. Annexes

Annex OMP 11-A	Security Authorities
Annex OMP 11-B	Table of Equivalent Security Classifications
Annex OMP 11-C	The Handling of OCCAR Restricted Information by Contractors
Annex OMP 11-D	Guidance Forms
Annex OMP 11-E	CIS Security Requirements for OCCAR Secret & Confidential Information
Annex OMP 11-F	CIS Security Requirements for OCCAR Restricted Information