



OCCAR Management Procedure

Title:	<u>Security Regulations</u>
Number:	OMP 11 Date: 02/02/11
Computer Ref:	OMP11_Security Regulations_issue6_020211
Current status:	Issue 6
Author/editor:	Elmar Kremer
Contact address:	Central Office, OCCAR-EA Bonn Tel: + 49 228 5502 121 Fax: + 49 228 5502 120 Email: elmar.kremer@occar.int
Endorsed by QMR:	(Original Signed) Eric Huybrechts, Deputy Director
Date:	02/02/11

Approved for issue: (Original Signed) Patrick Bellouard, OCCAR-EA Director Date: 02/02/11	OCCAR File Ref: CO/322/196/O-7
---	-----------------------------------

This document replaces: OMP 11 issue 5 dated 02/12/09

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 paragraph 6 and paragraph 12.2; revision of paragraph 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 Paragraph 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 paragraph 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 Paragraph 4.4.5.1; amendment of the provisions regarding RESTRICTED Information in Paragraph 5.1, 6.1, 7.1, 11.2 and 11.10 to adapt the Italian requirements.
01/12/10	6	Amendment of Paragraph 6.3.1 and 12.2.1, deletion of the definition of "Third Party", new provisions regarding USB memory sticks in Paragraph 9.3.3

Table of Content

<u>1. Basic Principles and Minimum Standards of Security.....</u>	<u>10</u>
1.1 General	10
1.1.1 Principles of Security in OCCAR	10
1.2 Personnel Security.....	10
1.2.1 Personnel Security Clearances.....	10
1.2.2 Security Instruction of Personnel.....	10
1.2.3 Security Status of Personnel	10
1.2.4 Denial of Access to Classified Information.....	11
1.3 Physical Security	11
1.4 Classified Information Entrusted to Contractor Facilities or Consultants	11
1.5 Release of Classified Information to Non-Programme Participating States	11
1.6 Measures to Counter Espionage, Sabotage, Terrorism/Safeguards Against Malicious Wilful Damage to OCCAR Bodies.....	11
1.7 Handling of NATO Classified Information	12
<u>2. Organisation of Security within OCCAR.....</u>	<u>12</u>
2.1 OCCAR Security Committee	12
2.2 Responsibilities of the OCCAR-EA Director	12
2.3 OCCAR-EA Internal Security Organisation	13
2.3.1 OCCAR-EA Security Officer	13
2.3.2 OCCAR-EA Programme Divisions	14
2.4 Security Inspections	14
<u>3. Security Classifications and Markings</u>	<u>14</u>
3.1 Levels of Classification.....	14
3.2 Classification Management.....	14
3.2.1 Application of Classifications	14
3.2.2 Downgrading and Declassification	15
3.2.3 "OCCAR" Markings	15
3.3 Access Limitations	15
<u>4. Transfer of Classified Information and Controlled Cryptographic Item (CCI) Material</u>	<u>15</u>
4.1 General	15
4.2 Packaging of Documents and Small-Sized Material	16
4.3 Transfer of Information Classified CONFIDENTIAL or SECRET within OCCAR Member States.....	16
4.4 International Transfer of Information and CCI Material Classified CONFIDENTIAL or SECRET and CCI Material between OCCAR facilities and its Member States and between OCCAR Member States.....	16
4.4.1 Transfer through Diplomatic channels	16
4.4.2 Transfer via commercial companies.....	17
4.4.3 Hand-carriage of Classified Information	17
4.4.4 Transfer CCI Material	18
4.4.5 Transportation of Items Classified CONFIDENTIAL or SECRET as FREIGHT by commercial carriers.....	18
4.5 Security Escorts	21
4.6 Transfer to Non-OCCAR Member States or International Organisations.....	22
<u>5. Personal Security Clearances.....</u>	<u>22</u>
5.1 General Requirements	22
5.1.1 Security Clearances for OCCAR-EA Staff Members and Personnel Temporary Employed by OCCAR-EA	22
5.1.2 Security Clearances for Contractor Personnel	23
5.1.3 Exchange of Information Affecting the Security Status of Personnel	23
5.1.4 Records of Access Authorisations / Personnel Security Clearances.....	24
<u>6. Access to Classified Information</u>	<u>24</u>

6.1	General Requirements	24
6.2	Access by Individuals holding the Nationality of an OCCAR Member State.....	24
6.3	Access by Other Nationals	24
6.3.1	Access by Nationals from Countries Participating in an OCCAR Programme.....	24
6.3.2	Access by Nationals from States not participating in an OCCAR Programme.....	25
6.3.3	Simplified Access to Classified Information.....	25
6.4	Consultation Process	25
6.5	Need-to-Know Decision	26
6.6	Security Instruction of Personnel.....	26
7.	<u>Industrial Security</u>	<u>26</u>
7.1	General Security Responsibilities	26
7.2	Contracts Involving CONFIDENTIAL or SECRET Information	27
7.2.1	Application of Security Classifications by Contractors.....	27
7.2.2	Pre-contractual Activities / Contract Negotiations / Invitations to Bid.....	28
7.2.3	Sub-contracts	28
7.2.4	Contract Security Clauses	29
8.	<u>Breaches of Security and Compromise of Classified Information</u>	<u>29</u>
8.1	General Responsibilities	29
8.2	Information to be Provided	30
8.3	Responsibilities for Investigations.....	30
8.4	Legal Consequences / Disciplinary Action.....	30
9.	<u>Protection of Classified Information Handled in Communications and Information Systems (CIS).....</u>	<u>30</u>
9.1	Scope.....	30
9.2	Security Objectives / Threats and Vulnerabilities of Systems	30
9.2.1	Loss of Confidentiality	31
9.2.2	Loss of Integrity.....	31
9.2.3	Lack of Availability	31
9.3	Minimum Security Requirements for Systems handling Classified Information	31
9.3.1	Technical Requirements	31
9.3.2	Administrative Measures.....	32
9.3.3	Physical Protection and Storage	34
9.3.4	Personnel Security	35
9.4	Systems-Specific Security Requirement Statement	35
9.5	Accreditation of Systems.....	35
9.6	Security Responsibilities.....	36
9.7	Requirements for Systems-Specific Security Operation Procedures	36
10.	<u>Visit Procedures</u>	<u>37</u>
10.1	Scope.....	37
10.2	Security Requirements for Visits.....	37
10.3	Visit Requests	37
10.4	Security Responsibilities.....	37
11.	<u>Handling of Restricted Information.....</u>	<u>38</u>
11.1	Applicability	38
11.2	Access	38
11.3	Release	39
11.4	Preparation and Marking.....	39
11.5	Handling and Storage.....	39
11.6	Reproduction and Destruction.....	40
11.7	Transfer	40
11.8	Use of IT-Equipment	40
11.9	Destruction and Maintenance of IT Systems and Equipment	42
11.10	Contracts Involving RESTRICTED Information.....	42

11.11	Loss, Unauthorised Disclosure or Violation of Procedures	43
11.12	Visits Relating to RESTRICTED Information.....	43
12.	Release of Classified Information.....	43
12.1	Release of Classified Information to OCCAR Member States not Participating in an OCCAR Programme.....	43
12.1.1	Release of Classified Programme Background Information.....	43
12.1.2	Release of Classified Programme Foreground Information	43
12.2	Release of Classified Information to Non-OCCAR Member States, International Organisations or Other Legal Entities	44
12.2.1	General Requirements from the OCCAR Security Agreement.....	44
12.2.2	Security Agreements or Arrangements	44
12.2.3	Sponsorship of Classified Information by an OCCAR Member State	45
12.3	Release Procedures	46
12.3.1	Classified Programme Background Information	46
12.3.2	Classified Programme Foreground Information.....	46
12.3.3	Denial of Release Approval	47
13.	Physical Security.....	47
13.1	Need for Protection	47
13.2	General Security Requirements	47
13.3	Minimum Requirements for Buildings housing Classified Information at CONFIDENTIAL OR SECRET Level	48
13.3.1	Construction of Buildings	48
13.3.2	Perimeter Fences	48
13.3.3	Guarding of Buildings	48
13.3.4	Access Control at Entries to Buildings and Parking Facilities.....	49
13.4	Basic Principles and Minimum Requirements for Access Control and Physical Security of Classified Information at CONFIDENTIAL or SECRET Level	49
13.4.1	General	49
13.4.2	Minimum Standards for Storage of CONFIDENTIAL or SECRET Information	50
13.4.3	Security Containers	50
13.4.4	Strong Rooms / Open Storage Areas	50
13.4.5	Security Areas and Administrative Zones	51
13.4.6	Guards / Other Response Forces.....	51
13.4.7	Control of Keys and Combinations.....	51
13.4.8	Physical Protection of Communication and Information Systems (CIS).....	52
13.4.9	Protection against Eavesdropping.....	52
13.5	Administrative Control of Classified Information or Material.....	52
13.5.1	General Requirements.....	52
13.5.2	Classified Registries and Archives	53
13.5.3	Classified Registers	54
13.5.4	Dispatching of Classified Information to External Recipients.....	54
13.5.5	Preparation of Classified Documents or Material.....	55
13.5.6	Reproduction	55
13.5.7	Destruction.....	56
13.5.8	Inventory Checks	56
14.	Annexes.....	57

List of Definitions

Board of Supervisors (BoS)	The BoS is the highest decision-making level within OCCAR. It directs and supervises the Executive Administration and the Security Committee.
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 by a security classification.
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 under the law of a Participating State obligating a Contractor or Sub-Contractor to furnish supplies or services in relation with an OCCAR Programme and that either will 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 personal 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 requirements prescribed for 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 Contract under the provisions of OCCAR Security Regulations, e.g. consultants, private companies.

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 is under security control of the respective NSA/DSA according to national laws and regulations, having employed security cleared personnel and, if appropriate, capability to handle and store classified Material up to a certain level (see Form OMP 11-05).
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)	The entity of the Government of each OCCAR Member State or Programme Participating State responsible 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 OCCAR Programme function.
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 Courier Certificate	Document provided to an individual appointed to carry a classified consignment according to the provisions of paragraph 4, which certifies that the bearer is authorised to carry the identified classified consignment and indicates details, schedule and route of the travel (see Form OMP 11-01 – OMP 11-04).

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 Nation or International Organisation under whose authority information has been produced or introduced into OCCAR
(Programme) Participating States	States participating in an OCCAR Programme and member of the relevant Programme Board.
Personal Security Clearance (PSC)	Certification issued by a NSA/DSA certifying that an individual holds a security clearance based on national security laws and regulations.
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)	Document issued by OCCAR-EA and approved by the Programme Participating States NSA's/DSA's describing the compulsory security provisions required for the performance of an OCCAR Programme, including details of classification, marking, handling, processing, safeguarding or transmission of Programme related Classified Information or Material. The PSI must include Security Classification Guides (SCG) and may include a transportation plan where appropriate. The provisions of a PSI may supplement the OCCAR Security Regulations 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)	Document issued by OCCAR-EA identifying those elements requiring security protection and the security classifications to be allocated to them.

Security Committee (SC)	Security Committee consists of nominated representatives of the NSA's/DSA's and chaired by an OCCAR Member State. It is responsible directly to the BoS for questions concerning OCCAR security matters and regulations.
Security Aspects Letter (SAL)	Document identifying the security requirements or those elements requiring security protection for an OCCAR Classified Contract
Sub-Contractor	A person or legal entity, which performs work under an OCCAR Programme in response to tasking or allocation of responsibility from a prime Contractor or another Sub-Contractor.

Related forms & templates

Form OMP 11-01	OCCAR Courier Certificates – Version I
Form OMP 11-02	OCCAR Multi Courier Certificates – Version I
Form OMP 11-03	OCCAR Courier Certificates – Version II
Form OMP 11-04	OCCAR Multi Courier Certificates – Version II
Form OMP 11-05	OCCAR FSC Information Sheet (FIS)
Form OMP 11-06	OCCAR Security Clearance Certificate
Form OMP 11-07	OCCAR Visit Request
Form OMP 11-08	Consultation Process
Form OMP 11-09	OCCAR Transportation Plan
Template OMP 11-10	OCCAR General Security Agreement
Template OMP 11-11	OCCAR Programme based Security Agreement
Template OMP 11-12	OCCAR General Security Arrangement
Template OMP 11-13	OCCAR Programme based Security Arrangement
Template OMP 11-14	Security Assurance
Template OMP 11-15	International Industrial Security Aspects Letter
Template OMP 11-16	OCCAR CCI Framework Transport Plan
Form OMP 11-17	Transport Announcement for Hand Carriage of Classified Material
Form OMP 11-18	Declaration by the Courier
Form OMP 11-19	Compromise or Possible Compromise Report Form
Template OMP 11-20	Security Assurance for RESTRICTED information

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 and uniform practices are applied.

1.1.1 Principles of Security in OCCAR

The principal objectives of security are to:

- safeguard Classified Information from espionage, compromise or unauthorised disclosure;
- safeguard important installations housing Classified Information from sabotage and malicious wilful damage;
- 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 NSA/DSA or where appropriate by the country of residency before such access is authorised. However, the Personnel Security Clearance for OCCAR Staff Members and other personnel temporarily employed by OCCAR-EA will 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 access to information classified CONFIDENTIAL or SECRET (e.g. messengers, security agents, maintenance personnel and cleaners, etc.), they must first be appropriately security cleared.

1.2.2 Security Instruction of Personnel

All personnel employed in positions involving access to Classified Information as stated under paragraph 1.2.1 above will 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 will 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 will 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 will meet the minimum standards for protection of OCCAR Classified Information as described in paragraph 13.

1.4 Classified Information Entrusted to Contractor Facilities or Consultants

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

1.5 Release of Classified Information to Non-Programme Participating States

Classified Information will 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 procedures as detailed in paragraph 12.

1.6 Measures to Counter Espionage, Sabotage, Terrorism/Safeguards Against Malicious Wilful Damage to OCCAR Bodies

In accordance with their national legislation the responsible security authorities of OCCAR Member States will provide to the OCCAR-EA Director or to his designated security organisation any intelligence or general information regarding espionage, sabotage, terrorism and other subversive activities to allow threat-assessment for OCCAR organisation and to enable OCCAR-EA to take the necessary precautions concerning:

- physical security measures for protection of Classified Information for OCCAR installations housing such information;
- the appointment and continued employment of international OCCAR-EA staff providing access to Classified Information or installations housing Classified Information;
- physical damage of OCCAR-EA premises;
- general safety of all OCCAR-EA staff and other national personnel permanently employed in OCCAR-EA Establishments;
- OCCAR-EA's essential functions to continue.

OCCAR-EA will refer to host nations for providing assistance and guidance in the fields of physical protection of OCCAR-EA Establishments and Classified Information held therein, counter measures against espionage, sabotage,

terrorism and safeguards against malicious wilful damage or any other criminal action. OCCAR-EA will also refer to host nations for providing adequate external protection to OCCAR-EA Establishments, including security of staff.

1.7 Handling of NATO Classified Information

NATO Classified Information released to OCCAR will bear the NATO classification (see Annex B) plus the distribution caveats "RELEASABLE TO OCCAR". That information must be protected and handled in accordance with these Security Regulations under the scope of the OCCAR-NATO Security Agreement.

2. Organisation of Security within OCCAR

2.1 OCCAR Security Committee

OCCAR Security Committee is responsible directly to the BoS for:

- examining questions concerning OCCAR security policy;
- considering security matters referred to it by the BoS, an OCCAR Member State or the OCCAR-EA;
- preparing appropriate recommendations to the BoS;
- proposing amendments and changes of the OCCAR Security Regulations.

The OCCAR Security Committee will consist of nominated representatives of the NSA's/DSA's and chaired by an OCCAR Member State.

If an OCCAR Member State appoints more than one representative it will nominate one as the official representative.

The OCCAR-EA Director or his authorised representative will attend each meeting of the OCCAR Security Committee.

The OCCAR Security Committee will meet once a year or upon request of one OCCAR Member State, the BoS or OCCAR-EA to discuss relevant matters of security.

The BoS will approve Terms of Reference and Rules of Procedure for the OCCAR Security Committee.

2.2 Responsibilities of the OCCAR-EA Director

The OCCAR-EA Director is responsible to the BoS for:

- enforcing the provisions of the OCCAR Security Agreement;
- applying these Security Regulations within OCCAR;
- considering security problems referred to him by the NSA's/DSA's of the OCCAR Member States;
- 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 will be responsible for:

- co-ordinating all matters of security within OCCAR, in particular issuing regulations for physical security measures including preparation, distribution, recording, reproduction, destruction, establishment of registries and storage of Classified Information within the OCCAR-EA;
- preparing specific PSIs and SCGs in consultation with the NSA's/DSA's concerned;
- 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;
- 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;
- requesting NSA's/DSA's of OCCAR Member States to provide Facility Security Clearances for Contractors or prospective Contractors;
- investigating or ordering an investigation into any leakage of Classified Information which, on prima facie evidence, has occurred in OCCAR-EA Establishments;
- 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;
- maintaining close liaison with all security authorities concerned in order to achieve overall co-ordination of security;
- 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 paragraph 2.2, the OCCAR-EA will have an internal security organisation, which will be equipped adequately with personnel resources.

The OCCAR-EA security organisation will 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 will also be responsible for the Communications and Information Systems and Network (CIS) within OCCAR-EA and will 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 Security Officer advises the OCCAR-EA Director on security matters and will 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 will 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 will 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 will be carried out either by the OCCAR Security Officer individually or together with the NSA/DSA concerned.

3. Security Classifications and Markings

3.1 Levels of Classification

The following security classifications will be applied:

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

Information will be classified only when necessary. The classification must be clearly and correctly indicated, and must be maintained only as long as the information requires protection.

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

3.2.1 Application of Classifications

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

For a given Document individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures may require different

classifications and will be marked accordingly. The classification of the Document as a whole will be that of its most highly classified part.

Other Material containing Classified Information must be marked in such a manner as to ensure that any recipient or viewer will know that Classified Information of a specified level is involved. The assigned security classification and, where appropriate, Downgrading and Declassification instructions will be conspicuously stamped, printed, written, painted or affixed by means of a tag, sticker, decal or similar device on classified Material.

3.2.2 Downgrading and Declassification

Classified Information may be downgraded or declassified only with the prior permission of the originator in writing and, if necessary, after discussion within OCCAR. The originator will be responsible for informing his addressees of the change, and they in turn will be responsible for informing any subsequent addressees, to whom they have sent or copied the Document, of the change.

Where appropriate, originators will specify on classified Documents or Material a date or period when the contents may be downgraded or declassified. Otherwise, they will keep the Documents or Material under review to ensure that the original classification still applies.

3.2.3 "OCCAR" Markings

"OCCAR" is a marking which, when applied to a Document or Material, signifies that the Document or Material is subject to the protective security measures outlined in these Security Regulations.

The marking "OCCAR" will be applied to SECRET, CONFIDENTIAL and RESTRICTED Documents or Material generated in connection with a specific OCCAR Programme or any OCCAR-EA activities.

3.3 Access Limitations

In cases where an OCCAR Member State or a State participating in an OCCAR Programme being the originator of information classified CONFIDENTIAL or SECRET, for security reasons, requires access to such information to be restricted to nationals of specific OCCAR Member States the Classified Information may be marked with an additional caveat (e.g. "XY Eyes Only").

Such Classified Information will not be released to OCCAR-EA.

4. Transfer of Classified Information and Controlled Cryptographic Item (CCI) Material

4.1 General

The provisions described hereafter apply to transfer of Classified Information at the CONFIDENTIAL and SECRET levels, as for CCI material, like documents, small sized Material or large volumes of classified material, including components or weapon systems.

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

- Government-to-Government channels, i.e. diplomatic pouch or military channels;
- security cleared government or company employees, or OCCAR-EA staff members acting as couriers following procedures as detailed hereafter;
- commercial courier companies (for CONFIDENTIAL), (any contractor planning to use commercial courier companies must first ask for prior approval from its NSA/DSA).

Programme 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.

4.2 Packaging of Documents and Small-Sized Material

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

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

The outer cover will bear a designation address and a package number for receipting purposes and will 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 will check the packaging for damage.

4.3 Transfer of Information Classified CONFIDENTIAL or SECRET within OCCAR Member States

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

4.4 International Transfer of Information and CCI Material Classified CONFIDENTIAL or SECRET and CCI Material between OCCAR facilities and its Member States and between OCCAR Member States

4.4.1 Transfer through Diplomatic channels

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

4.4.2 Transfer 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 transmitted via commercial courier companies, provided that the following criteria are met:

- 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;
- the courier company will obtain and provide to the consignor proof of delivery on the signature and tally record, or the courier must obtain receipts against package numbers;
- the courier company must ensure that the consignment will be delivered to the consignee prior to a specific time and date within a 24-hour-period under regular circumstances;
- 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.

4.4.3 Hand-carriage of Classified Information

In urgent cases information classified CONFIDENTIAL or SECRET which comply with the packaging requirements as described in paragraph 4.2 above may be transferred by hand provided that:

- the Courier holds the appropriate security clearance;
- the Courier is aware of his responsibilities for safe custody;
- the Courier must carry a Courier Certificate or a multi-travel Courier Certificate authorising him to carry the package as identified;
- a record of the information so carried is held in the appropriate registry of the dispatching facility.

The dispatching authority / facility will 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.

For hand carriage of Classified Information at CONFIDENTIAL or SECRET level 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.

Courier Certificates

For the hand carriage of Classified Information between OCCAR Member States by OCCAR-EA Staff and Experts or Government Representatives the Courier Certificate (Form OMP 11-01 and Form OMP 11-02) will be used.

For all other hand carriage of Classified Information at CONFIDENTIAL or SECRET level especially by Contractor personnel the Courier Certificate (Form OMP 11-03 and Form OMP 11-04) will be used.

The responsible NSA/DSA will issue or authorise the issuing of Courier Certificates for government representatives or Contractor personnel.

OCCAR-EA security officials will issue such Courier Certificates for OCCAR-EA staff or national experts seconded to OCCAR-EA.

4.4.4 Transfer CCI Material

CCI material will be transported by means that provide continuous accountability and protection against loss or unauthorised access during transit and intermediate stops.

Prior to a movement of CCI material, a transfer document (Form OMP 11-16) will be created by the consignor's Crypto custodian which will be transmitted to the consignor's NDA and through the consignee's NDA to the consignee's Crypto custodian. The CCI items will be delivered, as described below in this chapter, directly from the consignor industry to the consignee where its Crypto custodian will check the contents of the consignment against the transfer document. The receipted transfer document will be transmitted to the consignee's NDA and through the consignor's NDA to the consignor's Crypto custodian.

The package will not show externally any evidence of their CCI and/or Classified condition. It will be marked as CCI and/or with their classification internally.

The crypto keys must be properly erased before transporting CCI material (otherwise the classification of the material increases). In case of faulty equipment where it is not possible to guarantee the correct erasure of keys, the highest classification of the key must be applied to the contents of the consignment.

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

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

- The carrier company must be approved for the transportation of Classified Material;
- The carrier company must hold a Facility Security Clearance at the appropriate level, if required by national security laws and regulations;

- Where ever possible, consignments will be transported point-to-point;
- The consignor and consignee are responsible for jointly organising the transport including preparing a transportation plan (sample see Form OMP 11-09), and for its notification to and approval by their respective NSA/DSA prior to transportation;
- Where appropriate the NSA's/DSA's will advise their customs or other relevant national authorities of impending consignments and should be urged to give maximum priority to the shipment;
- Where possible the consignor must track the consignment in real time by a satellite positioning system.

4.4.5.1 By Road

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

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

4.4.5.2 By Rail

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

- Where necessary passenger accommodations should be made available for security guard personnel;
- 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.

4.4.5.3 By Sea

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

- 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;
- 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;
- 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;
- 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.

4.4.5.4 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:

- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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.

4.5 Security Escorts

Individuals fulfilling the duties of security escorts must be nationals of the Programme Participating States and be security cleared at the appropriate level.

The security escort must be composed of an adequate number of personnel to ensure regular tours of duty and rest. Their number will 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 will 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.

4.6 Transfer to Non-OCCAR Member States or International Organisations

International transfer of information classified CONFIDENTIAL or SECRET to a country, which is not a signatory of the OCCAR Convention or to an international organisation, will normally be by:

- Diplomatic Government-to-Government channels;
- Military Courier;
- Hand carriage;
- As freight by security cleared or approved commercial carriers subject to the requirements outlined in paragraph 4.4 above.

OCCAR and Non-OCCAR Member States or International Organisations may agree on other methods of transmission/transportation, if deemed necessary, and subject to the approval by the OCCAR Security Committee.

Where it is necessary to hand carry such Classified Information to Non-OCCAR Member States, if acceptable to the Non-OCCAR Member State concerned, the Courier Certificates (Form OMP 11-01 and Form OMP 11-02) and (Form OMP 11-03 and Form OMP 11-04) will also be used. However, if this is not acceptable the Courier Certificate will be agreed with the Non-OCCAR Member State concerned.

5. Personal Security Clearances

5.1 General Requirements

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

Personnel Security Clearances are not required for access to RESTRICTED information unless required by the States` national laws and regulations. If an OCCAR Member State or non Member State participating in an OCCAR Programme requires a Personal Security Clearance for access to RESTRICTED information, nationals without a Personnel Security Clearance from other States that do not require a clearance at RESTRICTED level must be granted access to such Information provided they have a Need to know.

5.1.1 Security Clearances for OCCAR-EA Staff Members and Personnel Temporarily Employed by OCCAR-EA

The clearance of OCCAR-EA Staff Members and personnel temporarily employed by OCCAR-EA will be the responsibility of the individual's respective national government based on national security laws and regulations.

This will 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 (see Form OMP 11-06).

NSA's/DSA's of the OCCAR Member States will issue security clearances for their national representatives in the BoS and provide the respective Security Clearance Certificates to the OCCAR-EA Security Officer. OCCAR-EA Security Officer will, on request, issue the relevant Assurances of Security Clearance according to the provisions of paragraph 10.

5.1.2 Security Clearances for Contractor Personnel

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

However, Personnel Security Clearances 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 will be undertaken by the competent security authority of that country conducting overseas checks as appropriate, and notifying the parent country.

A Personnel Security Clearance issued by one NSA/DSA will 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.

Personnel Security Clearances issued by the NSA's/DSA's of OCCAR Member States will 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 will 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.

5.1.3 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 effect the security of OCCAR-EA or one of its Member States, that Nation will 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.

5.1.4 Records of Access Authorisations / Personnel Security Clearances

All establishments handling information classified CONFIDENTIAL or SECRET will maintain a record of Personal Security Clearances granted for their personnel.

Each security clearance will 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 will be held by the responsible security officers.

6. Access to Classified Information

6.1 General Requirements

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

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

Personnel Security Clearances are not required for access to RESTRICTED information unless required by the States' national laws and regulations. If an OCCAR Member State or non Member State participating in an OCCAR Programme requires a Personal Security Clearance for access to RESTRICTED information, nationals without a Personnel Security Clearance from other States that do not require a clearance at RESTRICTED level must be granted access to such Information only provided they have a Need to know.

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, which does not bear a caveat as described under paragraph 3.3.

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

Individuals holding the sole nationality of an OCCAR Member State or the nationalities of both an OCCAR Member State, and a European Union country, and being employed in an OCCAR Member State, can have access to information classified CONFIDENTIAL or SECRET without the prior consultation with and approval of the originator.

The access by individuals holding the dual nationalities of both an OCCAR Member State and a Non-European Union country not participating in the relevant OCCAR Programme is covered in paragraph 6.3.2.

6.3 Access by Other Nationals

6.3.1 Access by Nationals from Countries Participating in an OCCAR Programme

Individuals holding the sole nationality of an OCCAR Programme Participating State or the nationalities of both an OCCAR Programme Participating State and a European Union country, and being employed in a OCCAR Programme Participating State can have access to Programme

Foreground Information classified CONFIDENTIAL or SECRET, relating to the Programme, which the State is participating, without the approval of the originator. However such individuals can have access to Background Information classified CONFIDENTIAL or SECRET only after consultation with and approval of the originator.

The access by individuals holding the dual nationalities of both an OCCAR Programme Participating State and a Non-European Union country not participating in the relevant OCCAR Programme is covered in paragraph 6.3.2.

6.3.2 Access by Nationals from States not participating in an OCCAR Programme

Individuals holding the nationality of a State that is not participating in an OCCAR Programme can only have access to Programme Foreground Information classified CONFIDENTIAL or SECRET after consultation with and approval of all countries participating in the OCCAR Programme concerned.

The decision for access of such individuals to Background Information classified CONFIDENTIAL or SECRET will rest with the originator.

6.3.3 Simplified Access to Classified Information

In order to simplify access to Classified Information, the Programme participants may agree, upon request of one of the participants, on a case-by-case basis and subject to NSA/DSA approval, that the access limitations in paragraph 6.3.1 and paragraph 6.3.2 may be less stringent. Such request will be given urgent consideration with the objective of reaching consensus. However, the adoption of a less stringent access policy will require the approval of all of the Programme participants.

6.4 Consultation Process

The consultation process concerning such individuals will be the following:

- The OCCAR Member States or OCCAR-EA, where appropriate, will notify and consult each other when access to Classified Information is required for individuals described under paragraph 6.3 above. This process will normally be initiated before the start or where necessary in the course of an OCCAR Programme;
- The information provided will be limited to the nationality of each individual concerned and the information to be accessed unless the OCCAR Member State receiving the notification requires more details or other relevant information on a case by case basis;
- The OCCAR Member State receiving such notification will examine whether access to its Classified Information by these individuals is acceptable or not;
- Such consultations will be given urgent consideration with the objective of reaching a consensus.

Where this is not possible the originator's decision will be accepted.

For the consultation process, OCCAR Member States will use the Form OMP 11-08.

If a positive answer cannot be given an exchange of views may take place between the requesting and the receiving NSA/DSA with the objective of finding a mutually acceptable solution.

6.5 Need-to-Know Decision

The Need-to-Know decision for OCCAR-EA Staff Members will be taken by the OCCAR-EA Director or, as appropriate, by the Head of the respective OCCAR Programme Division in co-ordination with the Security Officer or other designated OCCAR-EA security officials.

For Contractor personnel and OCCAR Member States' government agencies, the Need-to-Know decision will be taken by the responsible security officials.

6.6 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:

- the dangers to security arising from indiscrete conversation;
- precautions to take in their relations with the press;
- the threats, which may target the OCCAR-EA and its Member States;
- 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.

7. Industrial Security

7.1 General Security Responsibilities

For each OCCAR Programme OCCAR-EA will, in co-operation with the OCCAR Member States, prepare Programme Security Instructions (PSI) and associated Security Classification Guides and will determine, as appropriate, the specific security aspects of contracts let by OCCAR-EA requiring security protection and the security classification to be accorded to each aspect.

The Participant's relevant security authorities will be responsible for:

- The implementation of the PSI within their Government establishments involved in the Programme pursuant to the OCCAR Security Regulations; and
- Ensuring compliance with that PSI within industrial facilities.

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 will:

- Ensure that such Contractor(s), prospective Contractor(s), or Sub-Contractor(s) and their facility(ies) have the capability to protect the information adequately;
- Grant Personnel Security Clearances to all personnel whose duties require access to Classified Information in compliance with the provisions of paragraph 5.1;

- 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;
- Upon request of OCCAR-EA or any OCCAR Member State or other State participating in an OCCAR Programme grant a Facility Security Clearance to enable a company to negotiate or perform an OCCAR Classified Contract, sub-contract or call for tenders;
- Provide, upon request, to OCCAR-EA, an OCCAR Member State or any other State participating in an OCCAR Programme a Personal Security Clearance 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;
- Take action with regard to the specific arrangements to be carried out in matters of transportation in accordance with paragraph 4;
- ensure that, for any facility in which Classified Information is to be used, a person or persons are appointed to effectively exercise the responsibilities for safeguarding the Classified Information. These officials will be responsible for limiting access to the Classified Information involved in a contract to those persons who have been properly approved for access and have a Need-to-Know.

OCCAR Member States or any other State participating in an OCCAR Programme will 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 has been lost or disclosed to unauthorised persons. Each OCCAR Member State will comply with the investigative requirements in paragraph 8 of this Document.

7.2 Contracts Involving CONFIDENTIAL or SECRET Information

The contracts in an OCCAR-related Programme will be let by OCCAR-EA or OCCAR Member States according to the policies established in OCCAR. Sub-contracts will be let by the responsible contracting authority of a Contractor already engaged in the performance of an OCCAR contract or sub-contract.

7.2.1 Application of Security Classifications by Contractors

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

- The allocation of classification levels is the responsibility of the originator of the Classified Information;
- Classifications should be applied only to those aspects of a contract that must be effectively protected and such classifications should be strictly related to the degree of protection required;
- A compilation of information from more than one source will require co-ordination of the sources in the determination of the appropriate national or OCCAR classification levels;
- Provision should be made for Downgrading and Declassification as soon as this is possible;

- Changes in levels of classification should be made only with the permission of the originator.

The initial assessment of a level of classification of a contract where components are not defined and which involve the development of systems rests with the Contractor.

The levels of classification for possible sub-contracts will be based on the Programme Security Instruction, the Security Classification Guide or the Security Aspect Letter of the contracts to which they are related.

7.2.2 Pre-contractual Activities / Contract Negotiations / Invitations to Bid

Before negotiating an OCCAR Classified Contract involving access to information classified CONFIDENTIAL or SECRET, the responsible Security Officer of the establishment envisaging to let a Classified Contract or starting contract negotiations will request the NSA/DSA of the potential Contractor for a confirmation that the potential Contractor holds an appropriate Facility Security Clearance at least equal to the classification level of the information that will be required during the negotiation of the contract. The NSA/DSA will provide the Contractor or Sub-Contractor with the Facility Security Clearance.

For exchange of information relating to a Facility Security Clearance the Form OMP 11-05 will be used.

In case of bids, all invitations to bid in respect of OCCAR Classified Contracts will contain a clause requiring a prospective Contractor, who does not submit a bid to return all Documents which were provided to enable him to submit a bid to the contracting officer by the date set for the opening of bids. Similarly, an unsuccessful bidder will be required to return all Documents after a stipulated period of time (normally within 15 days after notification that a bid or negotiation proposal was not accepted).

7.2.3 Sub-contracts

After a contract has been let, it may become necessary for the Contractor to negotiate sub-contracts with Sub-Contractors to various levels.

All Sub-Contractors, in turn, may also negotiate sub-contracts with other Sub-Contractors and so on.

At whatever level it is proposed to negotiate a sub-contract, the following will apply:

- Before entering into negotiations, the Security Officer of the contracting authority will take the actions outlined in paragraph 7.2.2 above with respect to the potential Sub-Contractor, to its own NSA/DSA;
- In case the potential Sub-Contractor falls into the responsibility of another NSA/DSA, the NSA/DSA of the Contractor will issue the request to the former;
- The NSA/DSA of the potential Sub-Contractor will return the completed form together with the required information to the Contractor, following the same channels;

- Upon receipt of the assurance that the proposed Sub-Contractor holds a Facility Security Clearance or preliminary Facility Security Clearance to the required level the Contractor may open negotiations with the potential Sub-Contractor. It remains the responsibility of the NSA/DSA of the Sub-Contractor to make the appropriate arrangements to ensure the protection of all Classified Information issued to the latter;
- If a contract is subsequently let to a Sub-Contractor located in another OCCAR Member State, the Contractor placing the Contract will send one copy of the Contract security clauses and the SAL (OCCAR Template OMP 11-15) to its own NSA/DSA or Contracting Authority. That NSA/DSA or Contracting Authority will send the Contract security clause and the SAL to the NSA/DSA of the Contractor receiving the Sub-Contract, to enable the security requirements of the Sub-Contract to be monitored.

7.2.4 Contract Security Clauses

All Contractors and Sub-Contractors must be contractually required, under penalty of termination of their contract, to take all measures prescribed by their NSA/DSA for safeguarding Classified Information entrusted to, generated or manufactured by the Contractor.

Contracts placed with Contractors in OCCAR Member States or Non-OCCAR Member States participating in an OCCAR programme must include a security clause requiring the Contractor to comply with the OCCAR Security Regulations and the provisions of the Programme Security Instructions (PSI). The contract will also include a Security Aspects Letter identifying the classified aspects of the contract, in particular a Security Classification Guide or SCG issued from the Programme PSI SCG.

Contracts placed with Contractors in a Non-OCCAR Member State must include a security clause requiring the Contractor to comply with the national security laws and regulations for the protection of Classified Information of the country in which the Contractor is located.

Contractors or Sub-Contractors must place any further Sub-Contractor under appropriate security obligations no less stringent than those applied to his own contract or sub-contract.

8. Breaches of Security and Compromise of Classified Information

8.1 General Responsibilities

When OCCAR-EA or an OCCAR Member State or any other State participating in an OCCAR Programme discovers or is informed of a Breach of Security, compromise or loss of classified Programme information, they will take immediate action in order to:

- Establish the facts;
- Assess and minimise the damage done;
- Prevent a recurrence;
- Notify the appropriate authorities of the effects of the Breach of Security.

8.2 Information to be Provided

In case of compromise or loss of classified Programme information the following should be provided:

- A description of the information involved, including its classification, reference and copy number, date, originator, subject and scope;
- A brief description of the circumstances of the Breach of Security, including the date, the period during which the information was compromised and a statement of whether the originator has been informed.

8.3 Responsibilities for Investigations

A Breach of Security, compromise or the loss of Classified Information will be investigated by the OCCAR Security Officer, if it has happened within OCCAR-EA.

In other cases the NSA/DSA of the OCCAR Member State where the incident occurs will be responsible for the investigation.

The OCCAR-EA Security Officer will inform all NSA's/DSA's of the States participating in the Programme concerned about the results of its investigation and measures taken to prevent recurrences.

The NSA/DSA will inform the OCCAR-EA Security Officer and other NSA's/DSA's concerned about the results of its investigation and measures taken to prevent recurrences. OCCAR-EA will report all such cases to the BoS.

8.4 Legal Consequences / Disciplinary Action

Any individual, who is responsible for compromising Classified Information renders himself liable to disciplinary action.

Such action will not prejudice any legal action.

However, in respect of OCCAR-EA staff members and personnel temporarily employed by OCCAR-EA, reference is made to Article 3.1(a) of Annex I of the OCCAR Convention.

9. Protection of Classified Information Handled in Communications and Information Systems (CIS)

9.1 Scope

The security policy and minimum requirements described in this paragraph will apply to all official communications and information systems and networks - hereinafter called Systems - in which Classified Information at CONFIDENTIAL or SECRET level is processed, stored or transmitted.

Note: The security requirements for processing of RESTRICTED Information are detailed in paragraph 11.

9.2 Security Objectives / Threats and Vulnerabilities of Systems

Security measures established to protect Systems handling Classified Information must be designed to ensure Confidentiality, Integrity and Availability of the information handled therein, and to ensure the "Need-to-Know-Principle".

9.2.1 Loss of Confidentiality

Security measures established to ensure confidentiality of information handled in Systems must be designed to prevent unauthorised disclosure or compromise of the information.

Such unauthorised disclosure may be a result of:

- Activities of hostile intelligence services;
- Ordinary criminals activities (e.g. computer hackers);
- Disloyal staff;
- Failure of technical and administrative security precautions.

9.2.2 Loss of Integrity

Security measures established to ensure integrity of information handled in Systems must be designed to prevent accidental or deliberate corruption or alteration of the information as a result of activities as described under paragraph 9.3.1 below and / or malicious software or computer viruses.

9.2.3 Lack of Availability

Security measures established to ensure availability of information handled in Systems must be designed to keep the information rapidly accessible by authorised staff and to prevent the lack of availability of information as a result of activities as described under paragraph 9.3.1 below, malicious software or computer viruses and or/ failure of system hardware or software.

9.3 Minimum Security Requirements for Systems handling Classified Information

Confidentiality, integrity and availability of Classified Information handled in Systems may be achieved by technical, administrative, personnel and physical security measures established for the Systems as well as for and supporting system services and resources.

9.3.1 Technical Requirements

Systems handling Classified Information will meet the following minimum requirements.

9.3.1.1 General Hardware and Software Security Features

- Use of stand-alone computers, workstations, Local Area Networks (LANs) or portable CIS;
- Identification and authentication features with positive identification of all users at the start of each processing session (passwords, log-in, updated lists of authorised users);
- Automatic recording of all log on attempts, log off, initial creation, changes or withdrawal of access rights and privileges; initial creation or changes of passwords;

- Appropriate anti-virus protection (acceptable industry standard with regular software updates);
- Regular updates to operating system software;
- Proper data backup with secure local or external storage;
- General protection against emergencies and other potential damages or denial of operation (water, fire, power supply variations);

9.3.1.2 Tempest Protection

CIS and supporting devices (workstations, servers, printers, and monitors) will provide sufficient protection against compromising emanation in accordance with national security standards unless operated in an area, which is providing proper TEMPEST protection.

All hardware components providing TEMPEST protection will be subject to certification /approval by the competent national security authorities.

9.3.1.3 Communication Security

For transmission or exchange of Classified Information via accredited CIS encryption systems, devices will be used, which have been mutually accepted by the OCCAR Member States' NSA's/DSA's participating in a Programme.

OCCAR Security Committee may issue and maintain a mutually accepted list of approved encryption products.

For transmission of national Classified Information related to an OCCAR Programme within the territory of an OCCAR Member State only nationally approved encryption systems may be used.

However, in case of international transmission to Non-OCCAR Member States the encryption system will be mutually accepted by the NSA's/DSA's concerned.

OCCAR-EA will seek advice and technical support from the competent security authorities of the OCCAR Member State hosting OCCAR-EA Establishments, where necessary.

9.3.2 Administrative Measures

9.3.2.1 General Minimum Requirements

The following administrative measures will be put in place for systems handling Classified Information in Systems:

- Operation of Systems by authorised and trained personnel only;
- No use of privately-owned removable computer storage media and software (e.g. floppy disks, compact disks) or other IT hardware like laptops or PCs;
- Managed access to system and hardware components by security cleared personnel commensurate with the highest level of Classified

- Special application software in use to be verified at regular intervals by competent IT staff to ensure their integrity and correct functioning;
- Proper marking of hard-copy output and removable computer storage media;
- Records on Systems and user activity to be kept for a minimum of 2 years.

Since access to the Systems may allow access to Classified Information processed, stored or transmitted by the Systems records on user activity will also identify date and time of

- Access to files /folders containing Classified Information and
- Alterations of the contents of files.

9.3.2.2 System Installation / Operation

Systems will be operated by trained and competent and security cleared personnel duly authorised to access the Systems.

Any installation of hardware or software configuration of Systems will be carried out by security-cleared personnel only.

9.3.2.3 User Security Responsibilities

The personnel will be briefed on regular intervals about their specific security responsibilities related to the operation of the Systems.

Up-to date records about briefings received will be kept about all persons authorised to operate and use the Systems.

9.3.2.4 Incident Reporting

Users will be required to report all unusual incidents, which for instance may lead to potential vulnerabilities or a leakage of Classified Information to their competent security organisation.

9.3.2.5 Marking of Files Hardware and Printouts

Electronic versions of Documents or other forms of electronic records containing Classified Information, reproductions, extracts or derivatives and thereof containing such information will be classified and marked as stated in the Programme Security Instructions (PSIs) or Security Classification Guides to identify its classification and the originator.

For a given file the security classification will be indicated in bold and capital letters in red colour for SECRET and, where allowed under national security regulations, for CONFIDENTIAL or RESTRICTED in black colour, at the top and bottom of each page containing such Classified Information in written or other form.

All written pages will bear a page number.

Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures may require different classifications and will be marked accordingly.

Hard-Copy output or printouts may also be marked with appropriate stamps indicating the security classification.

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

9.3.2.6 Data Storage Media

Any removable data storage media containing Classified Information will be recorded in appropriate register books in accordance with the minimum requirements set out in paragraph 13.

9.3.2.7 Deletion / Destruction

Classified Information stored on Systems will be deleted by repeated overwriting.

At the end of their life-cycle, or for specific operational reasons, CIS, removable computer storage media such as diskettes or compact disks will be erased or destroyed otherwise in accordance with national rules and regulations or using appropriate destruction methods as described in Annex OMP 11-D.

9.3.2.8 Maintenance

All maintenance or repair work on Systems will be carried out by competent IT staff in areas with proper access control only.

In case repair cannot be carried out inside the user's facilities all data storage media must be removed and retained.

Contractor facilities involved in such repair or maintenance work of Systems will hold an appropriate Facility Security Clearance.

Any remote access or maintenance work is not permitted.

9.3.3 Physical Protection and Storage

Systems and supporting devices (workstations, servers, printers, monitors) processing or storing Classified Information will be protected by appropriate physical security precautions and access controls to prevent unauthorised persons from having access to the Systems or supporting components in accordance with the provisions of paragraph 13.

Systems permanently storing Classified Information will be located in dedicated security areas with a system of entry control, to include permanent protection during times the Systems are not operated.

Stand-alone PCs, laptops processing or storing Classified Information as well as removable computer storage media or hard-copy output containing such information will be stored in security containers or strong rooms in accordance with the provisions of paragraph 13.4.3 and 13.4.4.

Removable computer storage media (e.g. USB Memory Stick, external hard drives) which use an encryption system that has been accredited by one of the OCCAR Member States' NSA/DSA participating in the Programme and mutually accepted by the OCCAR Member States' appropriate Security Authority participating in the relevant Programme, will be handled in accordance with the applicable SecOps.

9.3.4 Personnel Security

All authorised users of Systems or maintenance personnel will also hold a security clearance of the appropriate level commensurate with the highest level of Classified Information processed stored or transmitted by the Systems, to include additional special authorisation for access to crypto Material, where appropriate.

9.4 Systems-Specific Security Requirement Statement

For all Systems handling Classified Information, a Systems-Specific Security Requirement Statement (SSRS) will be produced by competent security / IT security personnel.

As a minimum, the SSRS will describe in detail the following:

- The specific risks for the Systems;
- The operational environment of the Systems;
- The level and frequency of Classified Information to be processed, stored or transmitted;
- The nature of Classified Information (e.g. optical or acoustical signals, information in writing);
- The hardware and software configuration and features of the Systems and of supporting devices (system architecture);
- Software and hardware security features;
- TEMPEST and/ or COMSEC measures (including encryption systems used);
- Personnel, physical and administrative security measures;
- Security operating procedures or user instructions.

9.5 Accreditation of Systems

All Systems handling Classified Information will be subject to prior accreditation by the competent security authority based on the system-specific security requirements and technical features detailed in the SSRS.

Systems operated by OCCAR Member States' Government establishments or Contractor facilities located in OCCAR Member States will be accredited by the competent NSA/DSA.

Systems operated by OCCAR-EA and which are not connected to Systems operated by national Government establishments or Contractor facilities will be accredited internally by OCCAR-EA security organisation.

Systems operated by OCCAR-EA connected to national establishments or to Contractor facilities will be accredited by a joint panel of representatives of the NSA's/DSA's of the OCCAR Member States concerned and OCCAR-EA security experts.

For such Systems the SSRS also will be produced by the joint panel or a competent sub-group, as appropriate.

9.6 Security Responsibilities

For each System accredited for handling of Classified Information competent staff will be assigned to ensure:

- Compliance of the Systems with the security requirements, especially as specified in the SSRS; throughout the life-cycle;
- Implementation of administrative security requirements and Systems-specific Security Operation Procedures;
- Operational controls of security features.

The tasks may be carried out by competent IT security or INFOSEC experts.

9.7 Requirements for Systems-Specific Security Operation Procedures

Systems-Specific Security Operation Procedures will address the following issues:

- Scope of Document;
- Use of Systems for classified purposes;
- Approval / accreditation details;
- Location of Systems, security area;
- Physical protection, access controls;
- Personnel security requirements, visitors;
- Description of Systems and associated hardware and software (incl. Systems configuration) and mode of operation;
- Configuration management and administrator rights;
- Handling and protection of hardcopy output;
- Organisation of security and user management;
- User security responsibilities;
- General IT infrastructure and data backup;
- Emergency and contingency planning.

10. Visit Procedures¹

10.1 Scope

Subject to the provisions in paragraph 6 the arrangements described in this paragraph 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 will be described in programme PSIs.

10.2 Security Requirements for Visits

Such Classified Visits are subject to the following conditions:

- The visit has an official purpose related to OCCAR activities;
- The visitor has a Need-to-Know the information related to the specific OCCAR activity;
- The visitor(s) holds an appropriate Personnel Security Clearance;
- 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 will not be required.

10.3 Visit Requests

Prior to arrival at a facility identified under paragraph 10.1 above, information about the visitor will be provided directly to the receiving facility using the Form OMP 11-07 (OCCAR Request for Visit), by the Security Officer of the sending facility.

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 will 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.

10.4 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 paragraph 6, e.g. the consultation process, have been met.

¹ For visits relating to RESTRICTED Information only see Paragraph 11.

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

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

- Their name;
- The organisation they represent;
- Date of expiry of the Certificate of Security Clearance;
- The date(s) of the visit(s), and
- 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 will consult with OCCAR-EA or the NSA/DSA of the visitor.

11. Handling of Restricted Information

11.1 Applicability

Information classified or protectively marked RESTRICTED - hereafter also referred to as RESTRICTED Information and bearing an equivalent security classification marking will be protected as described hereafter.

11.2 Access

RESTRICTED Information will only be made accessible to OCCAR-EA Staff Members, Government representatives of the OCCAR Member States or Contractor personnel that require such information for performance of their official duties related to OCCAR ("Need-to-Know-Principle").

The contents of RESTRICTED Information must not be disclosed to the public, to any unauthorised persons or other legal entity.

All persons having access to RESTRICTED Information will be made aware of their responsibilities for the protection of such information according to these provisions and the consequences of negligence.

A Personnel Security Clearance or a Facility Security Clearance will not be required for access to RESTRICTED information unless required by the States` national laws and regulations. If an OCCAR Member State or non Member State participating in an OCCAR Programme requires a Personal Security Clearance or a Facility Security Clearance for access to RESTRICTED information, nationals without a Personnel Security Clearance and contractors without a Facility Security Clearance from other States that do not require a clearance at RESTRICTED level

must be granted access to such Information only provided they have a Need to know

11.3 Release

RESTRICTED Information will be released only to the Government establishments or Contractor facilities in the OCCAR Member States whose access is necessary in connection with their involvement in a specific OCCAR Programme or contract.

Release to any other Government, International Organisation or representatives thereof or to Contractors not located in an OCCAR Member State requires prior approval by the originator, if not stated otherwise in Programme specific arrangements.

11.4 Preparation and Marking

Documents or Material containing RESTRICTED Information or derivatives and reproductions containing such information generated or received will be marked or re-marked, as appropriate, to identify the RESTRICTED Information.

The originator will mark such information with a prefix to identify the origin.

All Documents or reproductions and extracts thereof containing RESTRICTED Information will be stamped, typed, printed or written in bold and capital letters at the top, and where appropriate for national RESTRICTED Information, at the bottom, of each written page and of all annexes containing such information.

Accordingly, reproductions of Documents or Material will be assigned the security classification and the marking of the original Document or Material.

Material or computer storage media and other optical, acoustical or electronic recordings containing RESTRICTED Information will 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 will know RESTRICTED Information is involved (e.g. by affixing a tag or sticker).

11.5 Handling and Storage

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

It must 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.

During travel the Documents must remain under the permanent personal custody of the holder and must not be left unattended in hotel rooms or vehicles and not be displayed in public.

RESTRICTED Information must not be downgraded or declassified without the prior written consent of the originator.

11.6 Reproduction and Destruction

Reproductions of RESTRICTED Information will be produced under conditions that can prevent unauthorised persons from gaining access.

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

To prevent unnecessary accumulation of RESTRICTED Information superseded or no longer needed, and provided there is no residual interest, RESTRICTED Information should be destroyed as soon as practicable or returned to the originator.

Documents or Material and computer storage media containing RESTRICTED Information should be reviewed at regular intervals to determine whether they can be destroyed.

11.7 Transfer

RESTRICTED Information will normally be transferred in a single envelope either by:

- Normal or registered mail, as appropriate;
- Commercial courier services;
- Personal carriage by staff members without formal Courier orders;
- The envelope must not bear a classification marking.

RESTRICTED Information must not be transmitted by communication systems or via the Internet unless an encryption system is used, which has been properly approved by an OCCAR Member State's security authority.

However, in exceptional circumstances telephone conversations, video conferencing or facsimile transmissions containing RESTRICTED Information may be in clear text, if an approved encryption system is not available, if time is of paramount importance, and provided that each occasion is explicitly authorised as applicable by the relevant Member State's NSA/DSA or OCCAR-EA security officials.

11.8 Use of IT-Equipment

RESTRICTED Information must be stored on stand-alone computers, which may only be accessed by staff members involved in the work under a given OCCAR Programme and having a Need-to-Know the information.

In Networks RESTRICTED Information must either be stored on individual home directories or on local group directories accessible to staff members only having a Need-to-Know the information.

Laptops storing RESTRICTED Information must be password protected and must not be directly connected to the Internet.

The following minimum-security measures must be in place when processing or transmitting RESTRICTED Information on IT systems:

- Managed access to system and hardware components (listing of persons authorised for access, storage in locked rooms);
- Proper identification and authentication features (passwords, log-in);
- Proper security monitoring and auditing;
- General protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations);
- Software versions (floppy disks, CD ROMs) in use must be checked for presence of malicious software or computer viruses before starting work on RESTRICTED Information;
- Removable computer storage media (e.g. floppy discs, compact disks) to be stored as described under paragraph 5 above;
- Proper data backup with secure local or external storage;
- Anti virus software (implementation, with updates, of an acceptable industry standard Anti-virus software);
- Such software must be verified at regular intervals to ensure their integrity and correct functioning;
- No use of privately-owned removable computer storage media and software (e.g. floppy disks, compact disks) or other IT hardware like laptops or PCs;
- No direct connection to Internet unless protected by firewall of an acceptable industry standard;
- Use of specific software tools designed for proper deletion of data;
- Proper instruction on the use of IT systems in place.

All systems must provide the following functionality:

- Up-to-date lists of authorised users;
- Positive identification of all users at the start of each processing session;
- Approved encryption systems/devices installed for the electronic transmission via public networks such as the Internet.
- Passwords should have a minimum of six (preferably nine) characters and include alphabetical, numeric as well as special characters.

Managed access to all systems or network processing or transmitting RESTRICTED Information must be in place to prevent any unauthorised access to systems or data.

The following events should be recorded:

- All log on attempts whether successful or failed;
- Log off, including time out where applicable;
- Initial creation, changes or withdrawal of access rights and privileges;
- Initial creation or changes of passwords.

Such records must be carried out by dedicated IT specialists only and be accessible to authorised personnel only. Copies of such records should be provided to responsible IT Security Staff, as appropriate.

Each page of hard-copy output or removable computer storage media must be marked with the RESTRICTED marking.

11.9 Destruction and Maintenance of IT Systems and Equipment

At the end of their life-cycle, or for specific operational reasons, removable computer storage media such as diskettes or compact disks will be erased, degaussed or shredded.

On fixed data media RESTRICTED Information must be deleted by overwriting after completion of work unless data is encrypted by means of approved encryption systems.

If deletion is not possible the data media will be removed and retained.

External facilities involved in the maintenance/repair work will be obliged, on a contractual basis, to comply with the applicable provisions for handling of RESTRICTED Information.

11.10 Contracts Involving RESTRICTED Information

All Contractors and Sub-Contractors must be contractually required, under penalty of termination of their contract, to comply with the security requirements for the handling of RESTRICTED Information as prescribed in this paragraph and as specified for Contractors in Annex OMP 11-C to the OCCAR Security Regulations.

Appropriate statements or supplementary documentation (e.g. "Security Aspects Letter"), identifying the information or those elements of the contract/sub-contract, which need to be classified RESTRICTED in accordance with the relevant "Security Classification Guide" for the Programme must be part of any contractual arrangement.

In case of bids, all invitations to bid in respect of a given OCCAR Programme involving RESTRICTED Information will contain a clause requiring a prospective Contractor who does not submit a bid to return immediately all Documents provided to him. Contractors/Sub-Contractors may acknowledge the security instructions for handling of RESTRICTED Information in a "bidding declaration", where applicable.

A Facility Security Clearance will not be required for Contractors/Sub-Contractors, which need access to RESTRICTED Information during the performance of contracts/sub-contracts or in pre-contractual stage unless required by the States` national laws and regulations. If an OCCAR Member State or non Member State participating in an OCCAR Programme requires a Facility Security Clearance for access to RESTRICTED Information, Contractors/Sub-Contractors without a Facility Security Clearance from other States that do not require a clearance at RESTRICTED level must be granted access to such Information provided they have a Need to know.

OCCAR-EA Security Office may, in co-ordination with the responsible NSA/DSA, conduct inspections at Contractor facilities to verify the implementation of the security requirements for the handling of RESTRICTED Information.

11.11 Loss, Unauthorised Disclosure or Violation of Procedures

Holders of RESTRICTED Information will investigate all cases in which it is known or there is reason to suspect that RESTRICTED Information has been lost or disclosed to unauthorised persons.

Any cases of loss, unauthorised disclosure of RESTRICTED Information or any violation of these regulations must be reported to OCCAR Member States' NSA's/DSA's concerned, OCCAR-EA and/or the originator of the information, as appropriate.

Actions may be taken by the relevant authorities, as deemed necessary.

11.12 Visits Relating to Information up to RESTRICTED

Visits requiring access to or discussion of up to RESTRICTED Information to government or commercial sites granted a Facility Security Clearance will be arranged directly between the sending and receiving establishments or facilities without formal requirements.

All visits to OCCAR-EA Establishments will be subject to notification to the security official of the respective OCCAR-EA Establishment prior to the visit taking place.

The sending establishment or facilities will provide to the receiving OCCAR-EA Establishment name(s) and details of the ID card(s) or passport(s) the visitor(s) will use for proper identification.

12. Release of Classified Information

12.1 Release of Classified Information to OCCAR Member States not Participating in an OCCAR Programme

12.1.1 Release of Classified Programme Background Information

Classified Programme Background Information will only be released to OCCAR Member States not participating in the Programme with the prior written consent of the originator.

Accordingly, any release of Classified Programme Background Information to Contractors or any other organisation located in such countries not participating in the respective OCCAR Programme will also require the prior written consent of the originator.

12.1.2 Release of Classified Programme Foreground Information

Classified Programme Foreground Information will only be released to OCCAR Member States not participating in the Programme with the prior written consent of all countries participating in the Programme.

Accordingly, any release of Classified Programme Foreground Information to Contractors or any other organisations located in OCCAR Member States

not participating in the respective OCCAR Programme will also require the prior written consent of all Programme participating countries.

12.2 Release of Classified Information to Non-OCCAR Member States, International Organisations or Other Legal Entities

12.2.1 General Requirements from the OCCAR Security Agreement

As required by the OCCAR Security Agreement any release of Classified Information to Non-OCCAR Member States, International Organisations, a legal entity not located on the territory of an OCCAR Member State or any other legal entity not involved in an OCCAR activity will be subject to the prior written consent of the originator of the information and an adequate Security Agreement or Arrangement.

Where the Classified Information to be released to a State not participating in an OCCAR Programme, International Organisations or a legal entity is not higher than the level of OCCAR RESTRICTED the “adequate Security Agreement or Arrangement” may be in the form of a written Security Assurance (Template OMP 11-20) signed by a representative duly mandated to commit the recipient State, International Organisation or other legal entity to protect OCCAR RESTRICTED information. The signatory must be an officially authorised representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity or a senior representative entitled to commit the entity he represents to protect OCCAR Restricted information. Where the RESTRICTED Information is to be released to a Contractor, a Security Assurance (**Template OMP 11-20**) will be obtained from the State where the Contractor is located and appropriate security conditions will be included in the Contract legally obligating the Contractor to protect the OCCAR RESTRICTED information.

The Security Assurance (**Template OMP 11-20**) shall be sent back to and registered by OCCAR-EA.

12.2.2 Security Agreements or Arrangements

12.2.2.1 Release of Classified Programme Background Information

Accordingly, OCCAR-EA is not permitted to release Classified Programme Background Information to a Non-OCCAR Member State, International Organisation or any other legal entity without the written approval of the originator and confirmation that an appropriate Security Agreement or Arrangement or an acceptable alternative exists.

An appropriate Security Agreement or Arrangement must be in place between the OCCAR Member State and a Non-OCCAR Member State, International Organisation or other legal entity to which Classified Programme Background Information is to be released. This also applies for the release of Classified Information to Contractors and any other organisations located in the Non-OCCAR Member State.

However, the originator concerned may approve the release of its Classified Programme Background Information to a Non-OCCAR Member State,

International Organisation or other legal entity without the existence of an appropriate Security Agreement or Arrangement.

12.2.2.2 Release of Classified Programme Foreground Information

The release of classified Programme Foreground Information to Non-OCCAR Member States, International Organisation or other legal entity not participating in a Programme will normally be subject to a Security Agreement or Arrangement that is authorised by the BoS and negotiated by OCCAR-EA with a Non-OCCAR Member State, International Organisation or other legal entity concerned which is based on one of the templates issued by the Security Committee.

When endorsed by the members of the Security Committee the final draft of a General Security Agreement or Arrangement (Template OMP 11-10) or (Template OMP 11-12) will be forwarded by OCCAR-EA to the BoS for final approval. In the case of a Programme specific Security Agreement (Template OMP 11-11) or Security Arrangement (Template OMP 11-13) it will be endorsed by the relevant members of the Security Committee and forwarded by OCCAR-EA to the BoS for final approval.

In the absence of a Security Agreement/Arrangement with a Non-OCCAR Member State that is to participate in an OCCAR Programme, when considered appropriate by OCCAR-EA, a separate Security Statement signed by a high-level Government representative of the Non-OCCAR Member State and OCCAR may be considered as sufficient to allow the release of Classified Programme Foreground Information to the Non-OCCAR Member State. The Security Statement must contain provisions similar to those contained in the templates of a Security Agreement/Arrangement (OMP 11-10/OMP 11-12) approved by the Security Committee. The final security provision in the Security Statement must be approved by the Security Committee members of the OCCAR Member States participating in the Programme. The Security Statement is Programme specific and cannot be used for the release of any Classified Information not related to the Programme Board Decision which the Non-OCCAR Member State has signed.

12.2.3 Sponsorship of Classified Information by an OCCAR Member State

In urgent circumstances where time does not permit the requirements of Paragraph 12.2.2 to be applied it may be possible for Classified Foreground Information to be released to a Non-OCCAR Member State participating in an OCCAR Programme under the sponsorship of an OCCAR Member State (the Sponsor) that is participating in the Programme subject to the following:

- A signed bilateral Security Agreement/Arrangement exists between the OCCAR Member State and the Non-OCCAR Member State recipient;
- The Sponsor will be responsible for obtaining a written Security Assurance (Template OMP 11-14) signed by a representative² duly

² The signatory must be an officially authorised representative who is either the direct recipient of the OCCAR classified information or is a senior representative from the NSA/DSA responsible for ensuring the protection of the information released in support of the OCCAR Programme

mandated by the recipient Non-OCCAR Member State. The Security Assurance (Template OMP 11-14) provided by the Non-OCCAR Member State **must** oblige the Non-OCCAR Member State to protect OCCAR Classified Information to a degree no less stringent than the provisions required by the recipient's national security laws and regulations and the provisions in the bilateral Security Agreement/Arrangement for the protection of the Sponsor's classified information. The OCCAR security classifications must be identified in the Security Assurance (Template OMP 11-14) with their equivalents to the national classifications cited in the bilateral Security Agreement / Arrangement;

- The Sponsor will provide the signed written Security Assurance (Template OMP 11-14) to the OCCAR-EA Security Office. A sponsor may present the Security Assurance to a Programme Participating State;
- Only information classified up to and including OCCAR CONFIDENTIAL may be released through the Security Assurance. Where there is a requirement to release OCCAR SECRET information to a Non-OCCAR Member State which has signed a Security Assurance (Template OMP 11-14) with an OCCAR Member State acting as Sponsor, OCCAR-EA must seek the agreement of the NSAs/DSAs of the Member States participating in the Programme prior to its release;

When OCCAR Classified Foreground Information is to be released to a Non-OCCAR Member State, International Organisation or other legal entity on the basis of a Security Assurance (Template OMP 11-14), OCCAR-EA must immediately initiate the negotiation of a Security Agreement/Arrangement with the Non-OCCAR Member State, International Organisation or other legal entity based on the security provisions contained in the template of a Security Agreement/Arrangement approved by the Security Committee.

12.3 Release Procedures

Unless stated otherwise in OCCAR Programme Security Instructions any release of Classified Information will be as described hereinafter.

12.3.1 Classified Programme Background Information

Requests for release of Classified Programme Background Information will be submitted directly to the originator's NSA/DSA indicated in Annex OMP 11-A or other responsible release authority identified in the relevant Programme Security Instructions, as appropriate.

Contractors or Sub-Contractors will submit such requests via their respective NSA/DSA.

12.3.2 Classified Programme Foreground Information

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

Sub-Contractors will submit such requests to OCCAR-EA via their contracting authority.

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

National Programme Co-ordinators will ensure the involvement of all appropriate national departments, including their NSA's/DSA's, in the decision making process.

If a decision on such release cannot be reached in the PC the issue will be referred to the OCCAR Board of Supervisors (BoS) for decision.

12.3.3 Denial of Release Approval

In case a State participating in the Programme cannot consent to the release of Classified Programme Foreground Information the reasons for the decision will be provided to the other Programme Participating States.

13. Physical Security

13.1 Need for Protection

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

13.2 General Security Requirements

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

Physical security precautions to be established for the protection of Classified Information in particular will 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 will 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.

13.3 Minimum Requirements for Buildings housing Classified Information at CONFIDENTIAL OR SECRET Level

13.3.1 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.

13.3.2 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 will 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).

13.3.3 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 will 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 will be determined according to the locally assessed threat and security environment.

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

13.3.4 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.

13.4 Basic Principles and Minimum Requirements for Access Control and Physical Security of Classified Information at CONFIDENTIAL or SECRET Level³

13.4.1 General

Classified Information at CONFIDENTIAL or SECRET level will 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 will be subject to continuous protection or periodic inspections.

Physical security precautions and technical equipment established for the protection of Classified Information will 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 enough time, almost any physical security measure is vulnerable to 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 will be evaluated against the time required to gain unauthorised access.

Response measures will 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.

³ For visits relating to RESTRICTED Information only see Chapter 11.

13.4.2 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 will be protected by one of the following methods:

- Continuous surveillance by guards or other duty personnel holding a security clearance of the appropriate level;
- Regular inspection of the security container by security cleared guards or duty personnel on a 24 hours basis;
- A nationally-approved intrusion detection system or closed circuit video system in combination with a response force that will, 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.

13.4.3 Security Containers

Security containers used for storage or archiving of Classified Information at CONFIDENTIAL or SECRET level will 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.

13.4.4 Strong Rooms / Open Storage Areas

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

- 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;
- Doors to be of solid construction in either wood or metal;
- Entrance doors to be secured with a built-in nationally approved three-position combination or similar lock;
- 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);
- 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;
- 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;
- 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

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.

13.4.5 Security Areas and Administrative Zones

All areas, where Classified Information is generated, transmitted or displayed otherwise will 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 paragraph 13.4.3 above.

13.4.6 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 will 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 will be tested and will be within a time limit evaluated as capable of preventing an intruder's access to the Classified Information being protected.

13.4.7 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, will not be taken out of office buildings.

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

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

Combination settings of security containers will 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 will be restricted to the smallest possible number of individuals.

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

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

Working and spare security keys will 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 will be held in sealed opaque envelopes by the local security managers.

Combination settings for security containers will be changed:

- On first being taken into use;
- Whenever a change of personnel possessing the combination occurs;
- Whenever a compromise has occurred or is suspected, and
- At intervals not exceeding 12 months.

13.4.8 Physical Protection of Communication and Information Systems (CIS)

Communication and information systems used for processing or transmission of Classified Information will 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 paragraph 9.

13.4.9 Protection against Eavesdropping

Areas in which information classified SECRET is discussed regularly will 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 or technical or physical security inspection of furniture and office equipment to be carried out by competent and authorised technical experts only.

OCCAR-EA may request assistance by experts from the competent National Security Authorities hosting OCCAR-EA Establishments.

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

13.5 Administrative Control of Classified Information or Material

13.5.1 General Requirements

Registry systems will 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

will be centralised to a maximum extent unless the amount of Classified Information or Material justifies decentralised management.

13.5.2 Classified Registries and Archives

Classified Registries will act as the main receiving and dispatching point for Classified Information or Material classified CONFIDENTIAL or SECRET and will 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 will be forwarded to external recipients via the Classified Registry only.

Registry Control Personnel will 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 will also be responsible for internal distribution and for keeping records of the location of each Document.

Classified Registries will be responsible to:

- Ensure the physical safeguarding of all classified Documents or Material at CONFIDENTIAL or SECRET level held by the Central Registry;
- 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;
- Maintain up-to-date records by name of all individuals authorized to have access to such Documents or Material held by the registry;
- Internally distribute such classified Documents or Material only to those individuals authorized to receive it;
- Dispatch externally such Documents or Material only addressees authorised to receive the Documents or Material;
- Ensure proper packaging and conformity with applicable requirements for transfer/transmission;
- Obtain receipts for all Documents or Material distributed internally or dispatched externally;
- Ensure a notice for a change in classification, Declassification or destruction certificate is held;
- Carry out inventories on an annual basis;
- Ensure classified Documents or Material accounted for is physically present and contain the correct number of pages.

Classified Registries will be established as a Security Area with a control of entry system, which will 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 will be protected in accordance with the standards set out in paragraph 13.4.2 and 13.4.3 above.

13.5.3 Classified Registers

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

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

- Internal register/serial number and classification level;
- Date of receipt;
- Date of creation of Document or Material;
- Originator and sender;
- Subject or title;
- Copy number;
- Number of annexes, if appropriate;
- Total number of pages / Material;
- Details of internal handling (destruction, Downgrading, creation of copies, internal);
- Details of dispatching to external recipients (date, copy number, recipient).

13.5.4 Dispatching of Classified Information to External Recipients

For any transfer of Classified Information or Material to external recipients the sending establishment will provide an appropriate dispatch note requiring the recipient to confirm the receipt. As a minimum, such dispatch notes will 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 will check with the responsible security authority whether the recipients hold a Facility Security Clearance at the appropriate level, in case recipients are industrial facilities.

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

For transfer of classified consignments via Government-to-Government channels Classified Registries will 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 will 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.

13.5.5 Preparation of Classified Documents or Material

Documents or Material containing Classified Information or derivatives and reproductions thereof containing such information will be marked to identify its classification and the originator, and as stated in Programme Security Instructions or Security Classification Guides.

The assigned security classification and, where appropriate, Downgrading and Declassification instructions will 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 will be marked accordingly.

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

Extracts from SECRET or CONFIDENTIAL Documents will 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 will be sought from the originator or other national classification authority for determination of the correct classification.

All classified Documents, copies or reproductions thereof will be conspicuously stamped, typed, printed or written in bold and capital letters in red colour and, where allowed under laws and security regulations, for CONFIDENTIAL or RESTRICTED level in black colour, at the top and bottom of the front cover or cover letter and each written page and of all annexes containing such information with the appropriate classification marking indicating the overall classification of the Document and each page thereof.

All written pages will bear a page number.

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 will 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 will know Classified Information is involved (e.g. by affixing a tag or sticker).

13.5.6 Reproduction

Any creation of copies or reproductions from CONFIDENTIAL or SECRET Documents or data storage media containing such Classified Information will 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 will 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) will 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 will 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 will be marked with identifying reproduction copy number.

The total number of reproductions, including reproduction copy numbers will 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 paragraph 9.

13.5.7 Destruction

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

Any such destruction will be carried out using nationally approved shredding machines or other methods as described in Annex OMP 11-D and for SECRET in presence of an authorised second staff member only.

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

13.5.8 Inventory Checks

Classified Registry Control Personnel will 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 will 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 will be carried out to verify:

- Consistency with information recorded in Register Books and physical presence of Documents or Material held within the registry;
- Physical presence of copy and destruction certificates;
- Physical presence of signed copies of dispatch notes/receipts for Documents or Material dispatched to external recipients;
- Evidence of tracer action taken and results thereof, in cases where such signed dispatch notes/receipts are not available.

14. Annexes

Annex OMP 11-A	Security Authorities
Annex OMP 11-B	Table of Equivalent Security Classifications
Annex OMP 11-C	Handling of Restricted Information by Contractors
Annex OMP 11-D	Destruction Methods for COSMEC Material / Data Storage Media