



## OCCAR Management Procedure

Title:	<b><u>Handling of Unclassified Sensitive Information</u></b>	
Number:	OMP 12	Date: 09/12/08
Computer Ref:	OMP12_Sensitive Information_Issue3_091208.doc	
Current status:	Issue 3	
Author/editor:	Elmar Kremer	
Contact address:	CSD, OCCAR-EA Bonn Tel: + 49 228 5502 121 Fax: + 49 228 5502 120 Email: <a href="mailto:elmar.kremer@occar.int">elmar.kremer@occar.int</a>	
Endorsed by QMR:	[Original Signed] Georges Peene, Deputy Director	
Date:	09/12/08	

Approved for issue:	OCCAR File Ref: CO/513/2491/Q-7
[Original Signed] Patrick Bellouard, OCCAR-EA Director Date: 09/12/08	

This document replaces: OMP 12 issue 2 dated 01/07/06

## Record of changes

Date	Issue	Changes
03/2001	OMP 4.6.2.4 Issue 1	Approved by the BoS on 15/12/00. Approved for issue by the Director of OCCAR-EA on 13/03/01.
14/02/05	OMP 12 Issue 1	Update of the OMP number in accordance with the structure of OMPs adopted by the BoS on 31/03/01. Application of the current OMP template.
01/07/06	2	Converted to the OCCAR-EA graphical house style
09/12/08	3	Review the document with the view to handle sensitive information in the same manner as RESTRICTED. Approved by 19 <sup>th</sup> BoS on 28/11/08.

## Table of Contents

<b><u>1. Introduction</u></b> .....	<b>4</b>
<b><u>2. Scope and Application</u></b> .....	<b>4</b>
<b><u>3. Basic Principles</u></b> .....	<b>5</b>
<b><u>4. Administrative Markings</u></b> .....	<b>5</b>
<b><u>5. Handling of Documents containing OCCAR Sensitive Information</u></b> .....	<b>6</b>
5.1 General Requirements .....	6
5.2 Marking of Information generated within OCCAR-EA .....	6
5.3 Marking of Information received from outside.....	6
5.4 Storage .....	6
5.5 Transmission .....	6
5.6 Addressing.....	7
5.7 Destruction .....	7
<b><u>6. IT Security</u></b> .....	<b>7</b>
6.1 Transmission .....	7
6.2 Processing .....	8
6.3 Marking .....	9
6.4 Deletion.....	9
6.5 Maintenance or any service related to Information Technology Systems:.....	9
<b><u>7. Release of OCCAR Sensitive Information</u></b> .....	<b>9</b>
7.1 Release of OCCAR Sensitive Information outside OCCAR-EA .....	9
7.2 Release of OCCAR Sensitive Information to other OCCAR Programme Divisions .....	9
7.3 Release of OCCAR Sensitive Information to Central Office.....	10
<b><u>8. Loss, Unauthorised Disclosure of OCCAR Sensitive Information or Violations of Handling Instructions</u></b> .....	<b>10</b>

## List of acronyms

BoS	Board of Supervisors
FTPC	Future Task and Policy Committee
FC	Finance Committee
SC	Security Committee
PC	Programme Committee
PB	Programme Board
CO	Central Office
IT	Information Technology

## 1. Introduction

Different kinds of sensitive information are circulating within OCCAR-EA to enable it to perform its tasks.

Information requiring protection in the interest of security of OCCAR or its Member States is so designated by the application of a security classification. The procedures for the handling of such classified information are described in the OCCAR Security Regulations (OMP 11) and subsequent security instructions to be applied by OCCAR-EA.

Other information relating to OCCAR Programme activities, which is not classified in the interest of security but otherwise defined as "sensitive", may also require protection and administrative control in the interest of OCCAR, whether such information originates in OCCAR-EA or is received from Member States or non-OCCAR sources.

## 2. Scope and Application

OCCAR Sensitive Information throughout this document means:

Any non classified information relating to OCCAR-EA or to a specific OCCAR Programme, which should not be released outside OCCAR-EA or to States (including OCCAR Member States) not involved in the programme or whose unauthorised disclosure would be disadvantageous to the interests of OCCAR, one of its Member States or any other originator of such information outside OCCAR.

OCCAR Sensitive Information is so designated by the application of Administrative Markings as stated under Paragraph 4 of this document. OCCAR Sensitive Information comprises, but is not limited to:

- Commercial or technical details of offers or contracts;
- Financial and accounting data for programmes (including price audits, price investigations, price analysis and synthesis, data and planning, detailed invoices);
- Programme decisions and reports to BoS, FTPC, FC, SC, PCs and PBs;
- Documents marked "**Commercially Sensitive**" or "**Commercial-in-Confidence**" or with any analogous marking.

This document establishes the principles and procedures to be applied for the protection and management of OCCAR Sensitive Information originated within OCCAR-EA or which is received from Member States or non-OCCAR sources.

It applies to OCCAR-EA and its Contractors. To this end, in any contract placed by OCCAR, OCCAR-EA shall make the provisions of this document applicable to Contractor and shall ensure that these provisions will be flowed down to all Sub-contractors, on the provisions of the Programme Security Instructions or on another contractual basis or otherwise. OCCAR Member States and Programme Participating States will also apply it when practicable.

### 3. Basic Principles

OCCAR Sensitive Information will be handled and stored in a manner to ensure its confidentiality and integrity, whilst allowing accessibility to staff members on a strict need to know basis.

It will:

- Be retained within the relevant Divisions ensuring the need-to-know principle;
- Be used for official purposes only;
- Be released in accordance with distribution limitations stated by the originator;
- Only made accessible to OCCAR staff members, Government representatives of the Participating States or contractor personnel that require such information for performance of their official duties related to OCCAR or a specific OCCAR programme, subject to the originator's stated distribution limitations and administrative markings and in accordance with the provisions of Para. 7 of this document;
- Be safeguarded or transmitted in a manner to prevent any unauthorised access;
- Not be made publicly accessible on the Internet or other public networks.

An accumulation of non-classified non-sensitive information may become OCCAR Sensitive Information when taken as a whole and justify the appropriate marking and protection.

People having access to OCCAR information shall be made aware that they shall in any case handle this information (even if unmarked) with due care regardless of its categorisation (unclassified, Sensitive Information or Classified Information).

### 4. Administrative Markings

In order to highlight the need to control dissemination of documents or other media containing OCCAR Sensitive Information to a specific group or staff members of OCCAR-EA, the originator of OCCAR Sensitive Information shall apply the marking except where paragraphs 5.3 apply.

**" XY SENSITIVE "**

with reference to a specific OCCAR programme or CO and indicating distribution or access limitations to specific group or individuals such as:

**"TIGER SENSITIVE – GERMAN/FRENCH/SPANISH EYES ONLY" or**

**"TIGER SENSITIVE – TIGER PD ONLY" or**

Markings may be combined or include release statements, e.g.:

**"FSAF SENSITIVE - RELEASABLE TO FRENCH/ITALIAN GOVERNMENTS ONLY"**

Markings may also be combined or indicate a date of expiry, e.g.

**"XY SENSITIVE - UNTIL ....."**

Such markings may only be modified by or with the consent of the originator, if not limited to a specific period of time.

## 5. Handling of Documents containing OCCAR Sensitive Information

### 5.1 General Requirements

Documents containing OCCAR Sensitive Information must be handled and stored in a manner to prevent unauthorised access.

Documents must remain under permanent personal custody including during travel and must not be left unattended in hotel rooms or vehicles and must not be read in public.

Additional requirements applicable to the release of OCCAR Sensitive Information are described in Para. 7.

### 5.2 Marking of Information generated within OCCAR-EA

All Documents and copies or reproductions thereof containing OCCAR Sensitive Information must be stamped, typed, printed or written in bold and capital letters at the top of each written page and of all annexes similarly sensitive (see Para. 4 above). Other media containing OCCAR Sensitive Information must be marked in such a manner that any recipient will know that Sensitive Information of a specific kind is involved (e.g. by affixing a tag, sticker). For computer storage media see Para. 6.

### 5.3 Marking of Information received from outside

Information which is received from outside OCCAR-EA bearing other markings to indicate a certain sensitivity, e.g. "**Commercially Sensitive**" or "**Commercial-in-Confidence**", shall be considered as OCCAR Sensitive Information without adding one of the marking described in Para 4 above. In case of doubt, consultation with the originator of such information will be necessary.

Such information will be afforded the same degree of protection as for OCCAR Sensitive Information originated within OCCAR-EA.

### 5.4 Storage

Documents containing OCCAR Sensitive Information which have been entrusted to staff to work on must not be left unattended or handled in a manner that could result in unauthorised access.

They shall be stored in locked desks, cabinets or similar containers or be secured in locked rooms/offices, provided that access to the room is limited to persons authorised to access them.

### 5.5 Transmission

OCCAR Sensitive Information will normally be transmitted in a single envelope by:

- Normal or registered mail, as appropriate
- Commercial courier services

- Personal carriage by OCCAR Staff without formal courier orders

In such cases the envelope must not bear any administrative markings as described under Para. 4 above.

OCCAR Sensitive Information may also be transmitted in double opaque, if deemed necessary. In such cases the inner envelope may bear administrative markings as described under Para. 4 above.

The originator may determine the means of transmission.

OCCAR Sensitive Information may also be transmitted via secure fax or e-mail connections approved for transmission of classified information at Restricted level or using an approved commercial encryption system for Restricted (see 6.1. and OMP 11 para.11)

OCCAR Sensitive Information must not be discussed over insecure telephone connections.

## 5.6 Addressing

However the recipient's address may indicate that the contents of the consignment only should be seen by and may directly forwarded to the individual to whom it is addressed, e.g.

**"PERSONAL for  
Mr./Mrs. XY  
at ..."  
+[XY Division], as appropriate**

+ mailing address

## 5.7 Destruction

To prevent the unnecessary accumulation of OCCAR Sensitive information, when it is superseded or no longer needed, provided it has no residual value, OCCAR Sensitive Information should be destroyed as soon as practicable. Holders will have to review documents on regular intervals to determine whether they can be destroyed.

OCCAR Sensitive 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.

Computer floppy disks or compact disks must degaussed, shredded or erased with a specific software tool designed for proper deletion of data (see also Para. 6).

## 6. IT Security

### 6.1 Transmission

OCCAR Sensitive Information may be transmitted via IT systems and networks which are using an encryption system properly approved by an OCCAR Member State's security authority.

## 6.2 Processing

OCCAR Sensitive Information should normally be stored or processed on IT-equipment with the following minimum security requirements implemented:

- 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 OCCAR Sensitive Information;
- Removable computer storage media (e.g. floppy discs, compact disks) to be stored as described under Para. 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 available.

Passwords should have a minimum of six (preferably nine) characters and include alphabetical, numeric as well as special characters.

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.

### 6.3 Marking

Each page of hard-copy output or removable computer storage media must be marked with the appropriate administrative marking as described under paragraphs 4 and 5 above.

### 6.4 Deletion

On fixed data media the Sensitive Information must be deleted by overwriting after completion of work with a special software tool unless the data are encrypted by means of approved encryption systems. If deletion is not possible the data media will be removed and retained.

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.

### 6.5 Maintenance or any service related to Information Technology Systems

Due to the quantity of Sensible Information contained in OCCAR IT systems, those systems are to be treated as if containing CONFIDENTIAL information for maintenance and service. In particular, to intervene on the IT equipments and systems, a service supplier staff (that is somebody working for OCCAR but not belonging to OCCAR permanent staff) shall respect the security clearance and nationality conditions described in OMP 11 paragraph 6 (to apply this, it will be considered that all OCCAR Programmes are concerned). Otherwise, a service supplier staff shall only intervene under the supervision or presence of an OCCAR IT staff member. Remote maintenance is forbidden.

## **7. Release of OCCAR Sensitive Information**

### 7.1 Release of OCCAR Sensitive Information outside OCCAR-EA

OCCAR Sensitive Information will only be released, on a strict need to know basis, to Nations, International Organisations or other legal entities not participating in the Programme with the prior written consent of the originator or of the Participating States and only after receiving the commitment from those legal entities to comply with the provisions of this OMP.

As a consequence, any release of Sensitive Information to Contractors located in such countries not participating in the respective OCCAR Programme will also require the prior written consent of the originator or of the Participating States.

### 7.2 Release of OCCAR Sensitive Information to other OCCAR Programme Divisions

Sensitive Information will only be released to other OCCAR Programme Divisions with the prior written consent of the originator or of the Participating States.

### 7.3 Release of OCCAR Sensitive Information to Central Office

In order to fulfil his responsibilities for the overall management of OCCAR-EA where necessary, the Director may have access to any kind of OCCAR Sensitive Information. Other Central Office staff Members may also have access to OCCAR Sensitive Information on a need to know basis, as authorised by the Director.

## 8. **Loss, Unauthorised Disclosure of OCCAR Sensitive Information or Violations of Handling Instructions**

Any cases of loss, unauthorised disclosure of OCCAR Sensitive Information or any violation of these Instructions will be reported immediately to OCCAR-EA Security Section and the BoS.

The OCCAR-EA Security Officer will notify the originator of the information about the loss or unauthorised disclosure.

Any Individual being responsible for violation of these Handling Instructions renders himself liable to disciplinary action. Such action will not prejudice any legal action.