



## OCCAR Management Procedure

Title:	<b><u>Handling of Restricted Information by Contractors</u></b>	
Number:	Annex OMP 11-C	Date: 08/03/10
Computer Ref:	Annex OMP11-C_Handling of Restricted Information by Contractors_issue5_080310	
Current status:	Issue 5	
Author/editor:	Elmar Kremer	
Contact address:	Central Office, 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:	<b>[Original Signed]</b> Eric Huybrechts, Deputy Director	
Date:	08/03/10	

Approved for issue:	OCCAR File Ref: CO/322/560/O-7
<b>[Original Signed]</b> Patrick Bellouard, OCCAR-EA Director	
Date: 17/03/10	

This document replaces: Annex OMP 11-C Issue 4 dated 01/10/08

## Record of changes

<b>Date</b>	<b>Issue</b>	<b>Changes</b>
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
01/10/08	4	Separation from the main document
08/03/10	5	Re-organisation of Paragraphs to be in line with the main document; amendment of the provisions regarding requirement of FSC/PSC.

## **HANDLING OF RESTRICTED INFORMATION BY CONTRACTORS**

### **1. Applicability**

This Document describes the handling of information classified or protectively marked RESTRICTED – (hereafter also referred to as RESTRICTED Information) - and which has been provided to a Contractor or Sub-Contractor pursuant to a contract let by OCCAR-EA.

This Document is also applicable to all phases of pre-contract activity, including solicitation (bids, quotations, and proposals), pre-contract negotiations or post-contract activity or repair and maintenance work requiring access to RESTRICTED Information or Material by a Contractor/Sub-Contractor or their personnel.

### **2. Access**

Information classified RESTRICTED will only be made accessible to Contractor personnel that require such information for performance of work under this contract (“Need-to-Know-Principle”). 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. Employees who, prove to be unsuitable for compliance with the provisions of this Document will be excluded from work on RESTRICTED Information.

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 provided they have a Need to know.

### **3. Release**

Except with the written consent given by the contracting authority the Contractor will not release RESTRICTED Information to any other persons other than employees of the Contractor or to any other third party and will not make use of any information or Material furnished by the contracting authority or produced on behalf of the contracting authority other than for the purpose of the contract.

### **4. Preparation and Marking**

For RESTRICTED Information or Material provided to him the Contractor must maintain the security markings assigned by the contracting authority or any other originator of RESTRICTED Information. Accordingly, copies and reproductions of Documents or Material will be assigned the security classification and the marking of the original Document or Material, if appropriate.

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).

## **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 permanent personal custody and may not be left unattended in hotel rooms or vehicles and may not be read in public.

RESTRICTED Information generated by or provided to the Contractor must not be downgraded or declassified without the written consent given of the contracting authority.

## **6. Reproduction and Destruction**

All Documents or Material, reproductions or extracts thereof containing RESTRICTED Information generated or produced by the Contractor 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.

RESTRICTED Information or Material, 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, provided there is no residual value, the Contractor must destroy such Documents or Material as soon as practicable or return them to the originator.

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

## **7. Transfer**

RESTRICTED Information must be transmitted in a single envelope either by normal or registered mail, commercial courier services or personal carriage by employees without formal Courier orders.

However, the envelope must not bear a classification marking.

The Contractor must transmit RESTRICTED Information via public network, e.g. by telephone, fax, video conferencing or email connections (including online services like www, ftp, telnet) only by using encryption systems properly approved by the respective National Security Authority (NSA) or Designated Security Authority (DSA), as appropriate.

In exceptional circumstances telephone conversation, video conferencing or fax transmissions may be in clear text, if approved encryption systems are 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.

## **8. Use of IT-Equipment**

The Contractor must have in place the following minimum security measures 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) are to be stored as described under Para. 6 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 functionalities:

- 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 accessible to authorised personnel only. Copies of such records should be provided to responsible IT Security Staff, as appropriate.

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

## **9. Destruction and Maintenance of IT Systems and Equipment**

At the end of their life cycle or upon termination of work under this contract, or as necessary for specific operational reasons, removable computer storage media such as diskettes or compact disks must 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.

RESTRICTED Information unencrypted on fixed data storage media must be deleted by overwriting using specific software tools available at IT Office prior to delivering IT equipment or components for maintenance or repair work outside access controlled areas or to Contractors.

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

External facilities involved in the maintenance/repair work must be obliged, on a contractual basis, to comply with the applicable provisions for handling of RESTRICTED Information as set out in this Document.

## **10. Contracts Involving RESTRICTED Information**

Prior to letting a sub-contract under this contract involving RESTRICTED Information the Contractor must seek approval from the contracting authority.

Sub-Contractors providing services or deliveries involving RESTRICTED Information must be contractually required to comply with the security requirements laid down in this Document.

All invitations to bid in respect of a potential sub-contract involving RESTRICTED Information must contain a clause requiring a prospective Contractor who does not submit a bid to return all Documents provided to him. Also an unsuccessful bidder must be required to return all Documents after a stipulated period of time (normally within 15 calendar days after notification that a bid or negotiation proposal was not accepted).

Sub-Contractors may acknowledge the provisions of this Document in a "bidding declaration", as appropriate.

Appropriate statements or supplementary documentation (e.g. Security Aspects Letter), identifying the information or those elements of the sub-contract, which need to be classified RESTRICTED, must be part of any sub-contract.

The Sub-Contractor's responsible security authority and/or representatives of the contracting authority may conduct inspections at Sub-Contractor facilities in order to verify the appropriate implementation of the security provisions laid down in this document.

All RESTRICTED Information generated or received in the performance of this contract must be returned to the contracting authority upon completion or termination of the contract, unless the information has been destroyed or authorised for retention.

Accordingly, the Contractor must return to the contracting authority or destroy all RESTRICTED Information relating to this contract not approved for retention. RESTRICTED Information approved for retention must be protected in accordance with the provisions of this Document and must not be used for other purposes without the prior written consent of OCCAR.

#### **11. Loss, Unauthorised Disclosure or Violation of Procedures**

The Contractor must investigate all cases in which it is known or there is reason to suspect that RESTRICTED Information provided or generated pursuant to this contract has been lost or disclosed to unauthorised persons.

The Contractor will promptly and fully inform the contracting authority of any relevant details of such occurrences. Action may be taken by the contracting authority in co-ordination with the Contractor's responsible security authorities, as deemed necessary.

#### **12. Visits Relating to Information up to RESTRICTED**

Visits requiring access to or discussion of up to RESTRICTED Information at 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 local OCCAR-EA Security Management prior to the visit taking place and providing the visitor's name and details of the ID Document(s) the visitor(s) will use for proper identification.