OCCAR Management Procedure

Title:	**Handling of Unclassified Sensitive Information**
Number:	OMP 12 Date: 19/07/17
Computer Ref:	OMP12_Handling of Unclassified Sensitive Information Issue4_20170719
Current status:	Issue 4
Contact address:	Central Office, OCCAR-EA Bonn Email: questions@occar.int

Approved for issue:	OCCAR File Ref: CO/PMSD/2017/00205

This document replaces: OMP 12 – Issue 3 dated 09/12/08

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 19th BoS on 28/11/08.
19/07/17	4	Complete rewrite; code of conduct introduction.

Table of Contents

List of definitions

Board of Supervisors (BoS)	The highest decision-making level within OCCAR which comprises of the ministers of defence or their delegates from each Member State. It directs and supervises the Executive Administration and the corporate committees.
Originator * **Only for the purpose of this document.*	A person or an entity by whose authority the information has been issued.
Removable Media	Any computer storage device designed to be removed from a computer without powering it down or affecting its operating state. The term includes CDs, DVDs, Blu-Ray Disks, Memory cards , Memory Stick etc., and other various types of storage device (Pen Drives, Hard Drives, Mobile Phones, Tablets etc) compatible with the Universal Serial Bus (USB), FireWire (IEEE 1394) and other interfaces.
Unclassified Information	Any information, document or material which has not been designated and marked with a security classification, as detailed in OMP11.
Unclassified Sensitive Information	Any Unclassified Information containing specific sensitivities relating to an OCCAR Programme, whose unauthorised disclosure would be disadvantageous to the interests of OCCAR, one of its Member States, OCCAR Programme Participating States or any other Originator.

List of acronyms

BoS	Board of Supervisors
CIS	Communication Information System
DDOS	Distributed Denial of Service
VTC	Video Tele-Conference

1. Basic Principles

1.1 General

These procedures lay down the basic principles and minimum standards of protection to be applied by OCCAR-EA and its contractors, so that it is assured that Unclassified Sensitive Information furnished or generated in connection with an OCCAR Programme or activity is appropriately protected.

In support of OCCAR-EA's activities, it is necessary to exchange large quantities of different types and forms of information; a significant quantity of which is sensitive in nature.

The most sensitive types of information – those which require protection in the interest of security of OCCAR, its Member States or OCCAR Programme Participating States – are designated by the application of appropriate security classifications. The procedures for the handling of OCCAR classified information are described in the OCCAR Security Regulations (OMP 11) and subsequent security instructions.

Other information relating to OCCAR which is not classified in the interest of security but is defined as "sensitive", also requires protection and administrative control. This is in the general interest of OCCAR, whether such information originates in OCCAR-EA or its contractors and subcontractors.

Unclassified Sensitive Information is so designated by the application of Administrative Markings as stated under paragraph 3 of this document. In general this comprises of 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);
- Documents marked in accordance with paragraph 3 of this document.

1.2 Code of Conduct

Underpinning these procedures is an agreed code of conduct that shall be observed by OCCAR Member States and Programme Participating States, such that a common understanding is established for the protection expected to be applied to Unclassified Sensitive Information furnished or generated in connection with OCCAR activities.

The underlying principle for the protection of Unclassified Sensitive Information is to ensure it is 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.

The primary objectives of the code of conduct are to ensure that Unclassified Sensitive Information will:

- Be used for official purposes only;
- Be used only for the purpose it was provided for;
- Not be released to third parties without the written consent of the Originator;

- Be released in accordance with distribution limitations stated by the Originator;
- Only be made accessible under a strict Need-To-Know principle and subject to the Originator's stated distribution limitations and administrative markings and in accordance with the provisions of paragraph 4.3 of this document;
- Be safeguarded from espionage, compromise or unauthorised disclosure, or transmitted in a manner to prevent any unauthorised access;
- Not be made publicly accessible on the Internet or other public networks.

People having access to Unclassified Sensitive Information shall be made aware that they shall in any case handle this information with due care.

1.3 Applicability

The Code of Conduct regarding the protection of Unclassified Sensitive information applies to all OCCAR Member States and Programme Participating States, in accordance with their own national regulations, when applicable.

The minimum standards of protection of Unclassified Sensitive Information as outlined in the remainder of these procedures apply to OCCAR-EA, its contractors, and sub-contractors.

2. Organisation of Security within OCCAR

2.1 Responsibilities of the OCCAR-EA Director

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

a) applying these protection requirements within OCCAR-EA;

b) considering security problems referred to him/her by relevant authorities of the OCCAR Member States;

c) examining questions involving changes of these security procedures, in close liaison with relevant authorities of the OCCAR Member States.

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

a) coordinating all matters regarding the protection of Unclassified Sensitive Information within OCCAR, in particular issuing procedures for physical and CIS security measures within the OCCAR-EA which are compliant with the provisions outlined herein;

b) ensuring that access to Unclassified Sensitive Information is limited to those personnel having a Need-to-Know for purposes on performance of OCCAR activities;

c) investigating or ordering an investigation into any leakage or possible leakage of Unclassified Sensitive Information which, on prima facie evidence, may have occurred in OCCAR–EA Establishments;

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

2.2 OCCAR-EA Internal Security Organisation

In order to fulfil the responsibilities mentioned in paragraph 2.1, OCCAR-EA shall have an internal security organisation, which shall be equipped adequately with personnel resources.

The OCCAR-EA security organisation shall be responsible for coordinating, supervising and implementing OCCAR security and verification of the enforcement of appropriate protective measures.

It shall also be responsible for the Communications and Information Systems (CIS) and Network within OCCAR-EA and shall co-ordinate the CIS matters within OCCAR-EA in co-ordination with relevant authorities concerned.

2.2.1 OCCAR-EA Security Officer

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

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

2.2.2 OCCAR-EA Programme Divisions

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

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

2.3 Security Inspections

Periodic inspections of the security arrangements for the protection of Unclassified Sensitive Information within OCCAR-EA shall be carried out either by the OCCAR Security Officer individually or together with the National authorities concerned.

3. Administrative Markings

Unclassified Sensitive Information will be distinguished by the marking "SENSITIVE" together with a subject reference. For a specific OCCAR programme this will include the Programme name, e.g. "PROGRAMME XY SENSITIVE". For general "OCCAR" or corporate information, this will be "OCCAR SENSITIVE". Industry shall mark their sensitive information accordingly, e.g. "[NAME OF THE COMPANY], [NAME OF THE OCCAR PROGRAMME] SENSITIVE".

When applied to a document, the application of the "SENSITIVE" signifies that the document is to be handled in accordance with the provisions of this OMP.

4. Handling of Unclassified Sensitive Information

4.1 General Requirements

Unclassified Sensitive Information must be handled and stored in a manner to prevent unauthorised access, compromise or unauthorised disclosure. As such, as a minimum, the procedures outlined in the following paragraphs shall be observed and implemented by OCCAR-EA, its contractors, and sub-contractors.

4.2 Access

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

Access to Unclassified Sensitive Information by contractors and/or subcontractors participating in the respective OCCAR Programme will require a contractual security clause or agreement for the protection of such information, in accordance with the procedures established in this OMP.

4.3 Release

4.3.1 Release of Unclassified Sensitive Information

Unclassified Sensitive Information will only be released, on a strict Need- to-Know basis, to States, International Organisations or other legal entities not participating in the Programme with the prior written consent of the Originator or of the Programme 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 Unclassified 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 Programme Participating States.

4.3.2 Use of Unclassified Sensitive Information in other OCCAR Programmes

Unclassified Sensitive Information related to one OCCAR Programme will only be used in another OCCAR Programme with the prior written consent of the Originator or of the original Programme Participating States.

4.3.3 Access to Programme related Unclassified Sensitive Information by Central Office

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

4.4 Storage

Documents containing Unclassified Sensitive Information 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 the documents.

4.5 Movement

The Originator may determine the means of movement however consignments containing Unclassified Sensitive Information shall be moved, as a minimum, either by:

- Normal or registered mail, as appropriate;
- Commercial courier services;
- Personal carriage without formal courier orders by government or company employees, or OCCAR-EA staff members.
- Electronic transmission by CIS as detailed in paragraph 5.2.4.

Single envelopes or packaging containing Unclassified Sensitive Information must not bear any administrative markings as described under Paragraph 3.

Unclassified Sensitive Information may be transmitted in double opaque envelopes, if deemed necessary. In such cases the inner envelope may bear administrative markings as described under paragraph 3.

When moving such consignments in person, documents must remain under permanent personal custody during travel and must not be read in public. However, for overnight stay in a hotel the consignment may be secured in a hotel safe.

4.5.1 Addressing

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

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

+ mailing address

4.6 Destruction

To prevent the unnecessary accumulation of Unclassified Sensitive Information, it shall be destroyed as soon as possible provided it has no residual value; such as when it is superseded or no longer needed. Holders of Unclassified Sensitive Information shall review documents at regular intervals in order to determine whether they can be destroyed.

Unclassified Sensitive Information, including interim material such as working drafts, shorthand notes, or spoilt copies shall be destroyed in a manner to ensure that they cannot be easily reconstructed.

Unclassified Sensitive Information stored on CIS storage media shall be deleted or destroyed as described in paragraph 5.2.

5. Communication and Information System Security

5.1 General Requirement

Unclassified Sensitive Information handled in electronic form on CIS shall be afforded protection from deliberate or accidental compromise, without inhibiting its use, specifically concerning:

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

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

For this purpose, a baseline set of protective measures has been developed by the OCCAR Member States which OCCAR-EA, its contractors and sub contractors shall observe and implement for the handling of Unclassified Sensitive Information within CIS.

It is not envisaged for CIS to undertake a formal approval process in order to handle Unclassified Sensitive Information. However, in accordance with paragraph 2.1, the OCCAR-EA Director shall be responsible for ensuring the protections are in place within OCCAR-EA' s scope of business.

5.2 Protective Measures

The protective measures outlined below must be applied within all OCCAR-EA, contractor or sub-contractor CIS intending to store, forward or process Unclassified Sensitive Information furnished or generated in connection with an OCCAR Programme or activity, in accordance with paragraph 1.1. Where exceptions exist, caution should be taken before allowing the CIS to handle such information.

To assist assessments, the measures are outlined in tabular format.

5.2.1 Identification, Authentication and Access Control

The need to know principle shall be enforced through the unique identification of individual users who have controlled access to information based on their job requirements.

ID	Requirement
1.1	All users shall be uniquely identified through the issue of personal account credentials prior to use of the CIS. User accounts with privileges (for System or Security Administrators, for example) shall be distinguished from normal user accounts and strictly controlled.
1.2	All users shall be authenticated by the CIS before any access to it is granted.
1.3	The use of previously-used passwords shall be prevented.
1.4	All passwords shall have a minimum time-period of validity.

ID	Requirement
1.5	Passwords shall be changed whenever they have, or are suspected to have been compromised or disclosed.
1.6	Administrator passwords shall be stored in a protected manner for emergency access (e.g. sealed in envelopes, locked in appropriate security containers) and shall be protected as Unclassified Sensitive documents.
1.7	Only limited feedback shall be provided to the user during the authentication process so as not to inform which aspect of authentication was incorrect.
1.8	Accounts that are no longer required shall be locked or deleted.
1.9	It shall be possible for the authentication process to be terminated for a particular user after an inappropriate number of failed login attempts.
1.10	All passwords shall have a minimum length of 9 characters, with a maximum time-period validity of 180 days.
1.11	Privilege-based mechanisms utilising Identification and Authentication data shall be implemented to restrict user access to only the information required to support a given programme or other OCCAR-related activity, taking into account the need-to-know principle.
1.12	Access to security and system information shall be restricted to only authorised security and/or system administrators.
1.13	The CIS shall lock interactive sessions after a specified period of user inactivity.
1.14	The CIS shall allow user-initiated locking of the user's own session, as defined above.
1.15	CIS and Storage Media used to store, forward, or process Unclassified Sensitive Information, shall be physically protected against unauthorised access.
1.16	Wherever possible, encryption systems shall be used to protect data-at-rest within Mobile Devices and removable storage media.

5.2.2 Security Management

Security mechanisms shall be implemented in order to detect, deter, and defend the system from deliberate and accidental malicious activity.

ID	Requirement
2.1	An audit log of security events shall be generated and maintained.
2.2	The audit trail and associated archive shall be protected from unauthorised deletion and/or modification, and shall be available in human-readable format.
2.3	Access to audit information shall be controlled; access permissions shall be established to permit access only by the appropriate management staffs.

ID	Requirement
2.4	Virus/malicious code detection software shall be installed. Wherever possible it shall be configured to automatically check on the introduction of removable media.
2.5	The virus/malicious code detection software shall be regularly updated.
2.6	Incoming e-mail, files, media and other exchanged data types shall be checked for the presence of malicious code.
2.7	Mechanisms shall be implemented which manage security functions and security-relevant data, which may only be performed or accessed by defined and authorised users (or roles).
2.8	CIS Security incidents shall be reported for inspection and investigation. This shall include notification to OCCAR-EA, and relevant National authorities wherever necessary.
2.9	Mobile Devices shall indicate discreetly to the user whether it is approved to handle Sensitive information or not.
2.10	Backup, recovery and business continuity requirements shall be considered.

5.2.3 Configuration Management

Processes shall exist that establish and maintain a baseline of controls within the CIS such that Unclassified Sensitive Information is afforded the same or a higher level of protection throughout use within the CIS.

ID	Requirement
3.1	Configuration baselines shall be established for all devices handling Unclassified Sensitive Information.
3.2	An inventory of hardware and software shall be maintained.
3.3	The installation and configuration of application software with security-relevant or security-enforcing functions shall be subject to a limited number of authorised system and security administrators.
3.4	Changes to the system or network configuration shall be assessed for their security implications / impacts.

5.2.4 Transmission

Provided that appropriate encryption systems are used (see below), OCCAR-EA, its contractors, and sub-contractors may transmit Unclassified Sensitive Information using any CIS – including public networks – in various data formats; such as fax, e-mail, voice call, Video Tele-Conference (VTC), Removable Media and direct file transfer.

The types of encryption system to be used will be determined by the authority responsible for authorising the use of the system (for example,

OCCAR-EA as contract authority). At the very least, encryption products used to protect Unclassified Sensitive Information shall make use of recent, relevant and active "state of the art" commercial cryptography standards (for example IPSec, TLS and SSH).

Systems approved to transmit OCCAR RESTRICTED information can also be used for the transmission of Unclassified Sensitive information.

ID	Requirement
4.1	Removable media used to store Unclassified Sensitive Information shall be marked in accordance with paragraph 3, in such a manner that any recipient shall know it contains Unclassified Sensitive Information (on the Material itself or on the container holding the Material).
4.2	Unclassified Sensitive Information shall not be transmitted via public network (e.g. by telephone, fax, Video Tele-Conferencing, E-mail, or via online services) unless an appropriate encryption system is used. Where exceptional urgent circumstances apply, Telephone conversations, video conferences, and facsimile transmissions containing Unclassified Sensitive Information may be conducted in clear text, subject to the following conditions: ▪ an appropriate encryption system is not available, and; ▪ time is of paramount importance, and; ▪ Unencrypted transmission of Unclassified Sensitive Information is not explicitly prohibited for the given OCCAR Programme or activity.
4.3	When Wireless LAN technology is used, the range of Access Points shall be set to minimise exposure to external attacks, with special attention given to the selection of antennae, their location, power and signal propagation.
4.4	The encryption used for transmission over Wireless LAN shall be in accordance with requirement 4.2

5.2.5 Physical Security

Each page of hard-copy output or removable computer storage media shall be marked with the appropriate administrative marking as described under paragraph 3.

ID	Requirement
5.1	Workstations, Mobile Devices, and removable media used to handle Unclassified Sensitive Information, and any hard-copy output shall be appropriately marked and protected.

5.2.6 Awareness and Training

A security education and awareness programme will emphasise the importance of information marking, labelling, and the balance between "responsibility-to-share" and "need-to-know".

ID	Requirement
6.1	Users shall be trained in the appropriate security actions they should be expected to perform, such as labelling/marking and dealing with a malicious software infection.

5.2.7 Maintenance, Repair, and Disposal of Equipment

Measures shall be implemented to protect equipment developed to store, forward or process Unclassified Sensitive Information during maintenance, repair, replacement, and/or disposal.

On fixed data media (including internal data storage and removable storage), Unclassified Sensitive Information shall be deleted by overwriting with commercial sanitisation tools.

Due to the quantity of Sensitive Information contained in OCCAR CIS systems, service supplier staff shall only intervene under the supervision or presence of an OCCAR IT staff member. Remote maintenance is forbidden unless appropriately supervised.

ID	Requirement
7.1	Equipment returning from external maintenance shall be subject to security checks and/or isolated testing prior to re-installation in the operational system.
7.2	Maintenance requiring remote access diagnostic procedures shall be permitted, albeit under strict control or supervision.
7.3	Equipment that has stored, forwarded or processed Unclassified Sensitive Information shall have its persistent storage overwritten using commercial sanitisation tools, unless appropriate encryption is used. Where this is not possible, the data storage shall be removed and retained.

5.2.8 Interconnection of CIS

CIS that intend to store, forward, or process Unclassified Sensitive Information may be directly or indirectly connected to other CIS – including public networks such as the internet – providing measures are established to ensure any Unclassified Sensitive Information being exchanged is appropriately protected.

ID	Requirement
8.1	Assets shall mutually authenticate with each other when establishing trusted connections in order to avoid communication with rogue devices masquerading as legitimate service providers.

ID	Requirement
8.2	Logical access control mechanisms shall be used to control local and remote access to data (this shall include boundary protection devices such as Firewalls).
8.3	The conditions and required actions for emergency disconnection/limitation of service(s) in the event of security incidents shall be established. This shall include the provision for protection against DDoS attacks.
8.4	Bidirectional end-to-end communication (such as voice over IP, collaboration, web conferencing and chat) over public networks shall be limited to UNCLASSIFIED conversations only, unless entirely contained within an appropriately encrypted connection.

6. Loss, Unauthorised Disclosure of Unclassified Sensitive Information or Violations of Handling Instructions

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

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

Any individual or entity being responsible for violation of these handling procedures renders himself/itself liable to administrative or contractual responsibility. Such action will not prejudice any legal action.