

**INTEGRATED AIR & MISSILE DEFENCE
CENTRE OF EXCELLENCE**

Souda Air Base, 73100, Chania

<http://www.iamd-coe.org>



Our Ref: NU. **TBD**

Tel.: +302821440738

NCN: 0302 615 4038

Date: **XX SEP** 2022

Email: info@iamd-coe.org

IAMD COE DIRECTIVE 25-01 (REV-1)

HANDLING OF DOCUMENTS

- REFERENCES:
- A. ACO Directive 70-1, Security
 - B. IAMD COE Directive 70-01, Security
 - C. IAMD COE Directive 35-01, Preparation of Correspondence

1. **Status.**

This is the 1st Revision of IAMD COE 25-01 Dir.

2. **Purpose.**

To state the policies, responsibilities and procedures governing the handling of documents.

3. **Applicability.**

This Directive applies to the IAMD COE Staff.

4. **Publication Updates.**

Updates are authorized when approved by the SC.

5. **Proponent.**

The proponent for this directive is the Director.

DISTRIBUTION:

Internal:

IAMD COE Staff via NU Intranet e-Library

TABLE OF CONTENTS

SUBJECT

PAGE

PARA

Policy	3	1
Responsibilities	3	2
Procedures	3	3

1. **Policy.**

1.1 Requirements for documents are to include the type of content, hardcopy or softcopy, cut-off date for electronic filing and destruction date.

1.2 Security handling of all documents is to be in accordance with Reference A and B.

1.3 Training is to be given to all newcomers after arrival. This includes best practices for the web service as maintained by the IAMD COE Security Officer. The staff is to be briefed about important changes to this Directive. Further training is to be provided as necessary to keep the staff proficient in handling documents

2. **Responsibilities.**

2.1 IAMD COE Registry personnel are appointed as Document Control Officer (DCO) and with the guidance and supervision of the CIS Staff of the Support Branch, they are responsible for training of all procedures of the staff.

2.2 Every office that handles documents, e.g., branches, project teams, is responsible for establishing its needs for documents.

3. **Procedures.**

3.1 **Creation of Documents.**

3.1.1 Files that are of official nature are to be created in accordance with Reference B and D. Registry is responsible for the issuing of file numbers in accordance with NATO policies. Users are to give files a meaningful name starting with "ddmmyy" where "dd" is the current day, "mm" is the current month and "yy" is the last two digits of the current year. File names are to show whether the document is in draft form. In "Properties", "Statistics", "Hyperlink base" links to the document are to be shown.

3.1.2 E-mail messages may be used to provide timely assistance to staff and management processes. They are not to be used to replace official messaging mechanisms, such as formal letters or signals. They are informal, unstructured (free format) messages which have no guarantee of delivery and which may be received by unintended addresses within the NATO Secret Wide Area Network (NS WAN) system. E-mail users are to maintain the normal proprieties of the military command structure; if one would not address a letter or make a phone call to an individual, then one should not send them an e-mail. The addresses of local (IAMD COE) and remote (NS WAN) users of the e-mail service are included in the Mail Address List.

3.2 **Releasing of Documents.**

3.2.1 Users are to use file numbers provided and maintained by Registry. If no appropriate file number is available a new one is to be requested.

~~3.2.2 Based on guidance from the Chief of Staff every Branch Head in his capacity as member of the IAMD COE is entitled to release unclassified / classified~~

~~documents including teletype messages of the precedence "R" "P" and "O". Signals with the precedence "Z" will be signed by IAMD COE Chief of Staff. Courtesy copies with the precedence "O" and "Z" should be provided to Directorate via Deputy Director. Other Staff Officers in the capacity as member of the IAMD COE are entitled to release unclassified / classified documents including teletype messages of the precedence "R" and "P". NCOs with rank of OR5 and higher are entitled to a precedence of "R". The list of authorized IAMD COE personnel to receive classified documents will be provided by Registry. Included in this list are Registry Members and Security personnel. Staff Officers acting in their capacity as "Senior National Representative (SNR) will be entitled to release messages with the precedence "R through Z" provided the release message indicates national business.~~

3.2.2 Internal and external e-mail attachments must not exceed a maximum file size of **10 MB**. To reduce storage capacity for staff internal mails, staff is encouraged not to use attachments, rather to use links or shortcuts. Extracts from any IAMD COE database are only to be included within e-mail messages following specific written authorization by the Branch Head or the Chief of Staff. Copies of released e-mail will be maintained automatically in individual "Sent Mail" folders. Users should consider placing a printed copy of released e-mail messages on relevant hardcopy files where this would help with the recording of activities on a particular topic.

3.2.4 Bulletin boards are to be moderated including comments. Briefings in the briefing generator are to be approved.

3.3 Handling of Documents.

3.3.1 All official documents both hard and soft copies addressed to IAMD COE are to be received through Registry.

3.3.2 IAMD COE email addresses are info@iamd-coe.org, registry@iamd-coe.org for NATO Unclassified documents and iamdcoe.registry@mod.grc.nato.int for NATO Classified documents.

3.3.3 Registry Personnel prints the daily inbox of all IAMD COE email addresses and forwards them hardcopy to the Directorate (DIR, DEP. DIR, COS). The Directorate writes at the first page any directions/orders and tasks the document/email to the appropriate office or Branch for information/action. The colors of pen for signature, comments, and ticks, are red for DIR, green for DEP. DIR and black for COS. Then, only if the document is NATO Unclassified, the Registry Personnel scans the first page, attaches it to the original email and forwards it according to the Directorate orders. The original hardcopy is registered to IAMD COE Registry Office. If the document is NATO Restricted, the IAMD COE personnel must be informed inside Class II areas and if it is NATO Confidential or above, inside Class I areas.

3.3.4 In case that an email sent to a staff officer (S.O) is relevant to IAMD COE and must be registered, the S.O sends it through his Branch Head or on behalf of him to IAMD COE email addresses according to classification, shortly explaining what it concerns about.

3.3.5 Mailboxes should be checked at least once per day. If users are away from their place to work for more than one working day, they are to activate the "Out of Office Assistant" or give another person delegate to access to their mailbox. If more than one user at IAMD COE receives an e-mail, especially with large attachments, the storing of this information should be internally coordinated to avoid duplication. Users should consider

placing a printed copy of incoming e-mail messages on relevant files where this would help with the recording of activities on a particular topic.

3.3.5 The Task Definition Report (TDR) and the Activity Report (AR) must be registered through Registry Office, after they are signed from IAMD COE Director. Then, the activity report, from all the SMEs must be gathered into one specific folder as an archive and later every year an IAMD COE annual (hardcopy) publication be created.

3.4 Storing of Documents

3.4.1 The filing system to store documents is to be the same for hardcopies as well as for softcopies. The CIS Staff of the Support Branch is to be responsible for the policy of the filing system. Registry is to administer the hardcopy system and CIS Office the softcopy system.

3.4.2 The top-level structures on the file and web server are managed by CIS Office and administered by Security Officer. Required changes are to be forwarded to the management. This part is to be kept under configuration control. Below users can freely structure their information maintaining management the principles of information management in IAMD COE. Users are encouraged to file e-mails that are of interest to other personnel or required to be kept for a long period of time on the file server rather than create sub-folders in the personal folder and file them there. Users should consider placing a printed copy of released e-mail messages on relevant files where this would help with the recording of activities on a particular topic. In general, it is recommended that messages should not be retained for longer than six months. Users are to update files on the web server when the original on the file server has been changed and there is no direct link.

3.4.3 Hardcopies are to be stored in accordance with their classification. Hardcopies of common interest are to be stored in Registry. All other hardcopies may be stored in the Branches.

3.5 Printing of Documents.

3.5.1 Printing is to be kept to the absolute necessary minimum to save resources.

3.5.2 Printed Classified Documents must be recorded in a logbook. The logbook is held by Registry Personnel.

3.6 Copying of Documents.

3.6.1 The normal way of changing the place of an object is to be copying and deleting the original to adopt privileges of the new location for the object. Users are to consider that hyperlinks and shortcuts to and from the object might be broken after the move.

3.6.2 Hardcopies and softcopies classified NATO ~~Secret~~ **Restricted and above** or registered by Registry are to be moved only through Registry.

3.7 Destruction of Documents

3.7.1 All destroyed documents are to be deleted in all instances where they are referenced.

3.7.2 Softcopies that are no longer required are to be deleted and destroyed. Files and folders are to be deleted. Deletion of Microsoft Outlook items will only move them to the "Deleted Items" folder. Therefore, the "Deleted Items" folder is to be

emptied latest when logging off. This feature is to be enabled in Microsoft Outlook. Web items are to be deleted. The Web Master is to destroy deleted items and pack the database at least once a month.

3.7.3 Hardcopies classified NATO Secret or registered by Registry are to be destroyed by Registry only. Users may destroy all other hardcopies classified NATO Confidential or NATO Restricted by using shredders and classified NATO Unclassified by putting them into the paper bins.

3.8 Management

3.8.1 It is recommended to do the following management actions in small portions on a regular basis, at least once a week. This will keep the amount of work small and support staff work continuously.

3.8.2 Users are to check their files at least once a year. Large files are to be compressed. Old files are to be cut-off or destroyed in accordance with the requirements for the documents. Duplicates are to be reduced as far as possible.

3.8.3 Users are to check their mailboxes at least once a month. Old items are to be deleted, if no longer required, or saved on the file server.

3.8.4 Users are to check their web items at least once a month. Outdated items are to be updated or deleted.

3.8.5 OPRs are to check their hardcopies at least once a year. Outdated items are to be destroyed.