MINISTRY OF DEFENCE

Secretariat General of Defence and National Armaments Directorate

Directorate of Air Armaments and Airworthiness

DEFINITION OF THE GENERAL REQUIREMENTS FOR REMOTE ACCESS TO THE INTERACTIVE ELECTRONIC TECHNICAL PUBLICATIONS (IETP) UNDER THE RESPONSIBILITY OF THE DAAA

NOTE

This Technical Publication (TP) cancels and replaces its previous edition dated 15/04/2008 and the related supplement "A" dated 09/02/2012

Basic Edition: 14/05/2014

English Edition: 25/03/2019

LIST OF EFFECTIVES PAGES

ATTENTION: This regulation is valid if composed by the pages listed below and duly updated.

Copy of this regulation may be found at the address:

http://www.difesa.it/SGD-DNA/Staff/DT/ARMAEREO/Biblioteca/Pagine/default_.aspx

The issue dates of the original and amended pages are:

Original………………………0 ……………………..of 25/03/2019

This regulation consists of a total of 11 pages as specified below:

Page No.	Amendment No. .
Frontpage	……. 0
A	……. 0
I .	……. 0
1-8	……. 0

TABLE OF CONTENTS

1 OVERVIEW

This regulation establishes the general requirements for accessing Interactive Electronic Technical Publications (IETPs) of DAAA responsibility via Wide Area Network links.

Whenever data networks shall be used to manage classified information, these shall be approved beforehand, in terms of their security aspects, by the ANS. This approval shall be extended to the EDP systems connected to the same Data Networks.

For the classification of IETPs under DAAA responsibility, refer to the regulation AER(EP).P-170.

1.1 TASKS AND SCOPE

Although most of the requirements have been formulated to ensure maximum applicability to all IETP classes, there are some requirements with applicability only to IETP classes X and XP.

For this reason, the requirements concerning Configuration Control have been divided into two different sections – 2.1 and 2.2 – depending on the class of IETP they apply to. Sections 2.3, 2.4 and 2.5, on the other hand, contain requirements common to all IETP classes.

Implemented solutions are not exempt from data security classifications, which are obviously more easily applied to data with low security classification.

This regulation assumes the possibility for almost complete transmission of IETPs, with security classification up to RESTRICTED, via data networks approved by the ANS in accordance with (i.a.w.) the applicable security directives as per section 1.2.

IETPs with security classification above RESTRICTED will be stored on media defined in security directives concerning distribution and management of classified EDP as per section 1.2.

The configuration provided for is Client with dedicated software-Server or commercial Browser-Server. In exceptional cases only (e.g. War Time), due to absence or discontinuity of communication networks, there may be local installations operating as Servers, regulated via standards adapted to the contingent situation.

1.2 APPLICABLE STANDARDS

AER(EP).0-0-2 Definizione e Regolamentazione del Sistema delle Pubblicazioni Tecniche della Direzione degli Armamenti Aeronautici (Armaereo) – Herein translated into: "*Definition and Regulation of the Directorate of Air Armaments (Armaereo) System For Handling Technical Publications*"

AER.0-0-8	Norma per le Pubblicazioni Tecniche – Emissione, compilazione ed inoltro delle "Segnalazioni Inconvenienti Pubblicazioni" (S.I.P.), concernenti le Pubblicazioni tecniche Aeronautiche di competenza di Armaereo – Herein translated into: "*Issuing, Filling in and Forwarding of the "Technical Publications Occurrence Reports", concerning the Armaereo's Aerospace Technical Publications*"
AER(EP).00-00-5	Controllo configurazione. Processi per l'elaborazione, valutazione, ed autorizzazione delle modifiche da introdurre nei materiali di competenza della D.A.A.A. – Herein translated into: "Configuration Control. Process for Preparation, Assessment and Approval of Configuration Changes to DAAA's materials"
AER.00-00-6	Individuazione e Registrazione della Configurazione degli Articoli Aeronautici – Linee Guida per le FFAA e CdS – Herein translated into: "Identification and Registration of Aeronautical Configuration Items – Guidelines for Armed Forces and State Corps"
AER.P-101	Requisiti generali di stile e presentazione per la preparazione degli esecutivi dei manuali tecnici – Herein translated into: "General style and presentation requirements for preparing print-ready technical manuals"
AER(EP).P-104	Emissione ed aggiornamenti dei Manuali Tecnici accettati dalla D.A.A.A. – Herein translated into: "Issuing and updating Technical Manuals accepted by the DAAA"
AER(EP).P-170	Definizione dei requisiti generali delle pubblicazioni tecniche elettroniche interattive (IETP) della D.A.A.A. – Herein translated into: "Definition of the general requirements of Interactive Electronic Technical Publications (IETP), responsibility of the DAAA"
AER(EP).P-171	Definizione dei requisiti generali delle pubblicazioni tecniche elettroniche interattive di classe P (IETP-P) di competenza della D.A.A.A. – Herein translated into: "Definition of the general requirements of Interactive Electronic Technical Publications Class P (IETP-P), responsibility of the DAAA"
AER.P-172	Definizione dei requisiti generali delle pubblicazioni tecniche elettroniche interattive di classe L (Strutturate linearmente) di competenza di ARMAEREO – Herein translated into: "Definition of the general requirements

of the Interactive Electronic Technical Publications Class L (with linear structure) responsibility of ARMAEREO"

AER.P-173	Definizione dei requisiti generali delle pubblicazioni tecniche elettroniche interattive di classe X (ottimizzate per reti intranet/internet di competenza di ARMAEREO – Herein translated into: "Definition Of The General Requirements for The NATO AGS Interactive Electronic Technical Publications (IETP), responsibility of ARMAEREO"
AER(EP).P-174	Definizione dei requisiti generali delle pubblicazioni tecniche elettroniche interattive (IETP) di classe XP di competenza della D.A.A.A. (ottimizzate per reti Internet e derivate da formati originali vari) – Herein translated into: "Definition of the general requirements of Interactive Electronic Technical Publications (IETP) Class XP, responsibility of the DAAA (optimized for the Internet and deriving from various original formats)"
AER.Q-2010	Processo di valutazione dei sistemi di gestione per la qualità dei fornitori della D.A.A.A. – Herein translated into "Evaluation process of DAAA suppliers' quality management systems"
PCM ANS 2/R/2006	Disposizioni in materia di sicurezza delle comunicazioni classificate e procedure per il servizio cifra – Herein translated into "Directives on the security of classified communications and procedures on the crypto service"
PCM ANS 5/2006	Disposizioni in materia di sicurezza dei sistemi per l'elaborazione automatica dei dati classificati – Herein translated into "Directives on the security of the systems for Automatic Classified Data Processing"
PMC ANS 6/2006	Misure di sicurezza materiale per la salvaguardia delle informazioni classificate – Herein translated into: "Security measures on the material for the protection of classified information"
DPCM 03/02/2006	Norme unificate per le protezione e tutela delle informazioni classificate – Herein translated into: "Unified regulations for the protection of the classified information"

1.3 REFERENCE STANDARDS

S1000D International Specification for Technical Publications Utilizing a
Common Source Data Base

1.4 DEFINITIONS OF TERMS AND ACRONYMS USED

Refer to standard AER.Q-2010 for the definitions of acronyms, terms and expressions used in this regulation with the exception of the following peculiarities.

1.4.1 Interactive Electronic Technical Publications (IETP)

These are publications which can be viewed using a computer system and which permit direct access to the information contained within via multimedia and/or hypertext navigation functions i.a.w. their class.

1.4.2 Local Area Network (LAN)

This is a collection of computers and peripherals directly and permanently connected in order to exchange data and share peripherals. A dedicated computer (Server) manages the data traffic across the network.

1.4.3 Wide Area Network (WAN)

This is a network which connects LANs in different geographical locations. The connection, permanent or occasional, is made via modems, fixed lines and radio or satellite bridges. Multiple Servers are used, one for each data network.

1.4.4 Peculiar Acronyms

ANS   *Autorità Nazionale per la Sciurezza* – National Security Agency

EDP   *Elaborazione Automatica e/o elettronica di Dati* - Automatic and/or Electronic Data Processing

PC   Personal Computer

1.5 APPLICABILITY

This AER(EP).P-175 enters into force from the date of its approval.

2   REQUIREMENTS

2.1 CONFIGURATION CONTROL OF CLASS P AND L IETPS

There is a single site (the server) managed by the Company which supplies the IETP (the Company) to where the latest official version of the Publications is made available to the user that can view them by means the applicable software (the Client with dedicated SW or commercial browser). One or more persons (the Administrators) are responsible for managing and monitoring the distribution Server for this site.
The administrators contribute to preparing the IETP User manual.
The manual covers all aspects concerning the methods of processing and viewing the data contained in the IETPs, via network.

In the same way, on the User side there shall be an appropriate control policy which includes an Administrator with the task of supervising installations and Users.

The IETPs shall be protected in order to avoid modification of the data stored on the Server. It is the Company's responsibility to ensure the integrity of the data stored on the server and protect them against unauthorized modification.

The Server shall contain an on-line help menu listing complete procedures.

This will include step-by-step instructions for correct Client installation, when required.

If the Client can be installed on different operating systems, a procedure shall be prepared for each individual operating system.

Users shall be notified automatically of the presence of new Modifications on the site via on-screen notifications (e.g.; pop-ups).

In addition, whenever possible, any modifications shall be indicated by the Client (the Client with dedicated SW or commercial browser), as described later in this regulation.

The Client (the Client with dedicated SW) downloaded from the server shall only allow access to data via authentication.

The Client (the Client with dedicated SW or commercial browser) shall not allow any modification to be made to the individual DMs / IETPs stored on the Server.

Any addition of bookmarks or notes shall be managed via separate saved either locally or on the server.

The Client (the Client with dedicated SW or commercial browser) shall:

➢ Highlight, at the start of each connection, the presence of an entire new edition or updates to the IETP being viewed, via notifications on screen via pop-up, with respect to the last access made by the User;

➢ Place identifying data on each hardcopy printout requested by the User, in compliance with the regulation AER(EP).P-170.

The individual DMs / IETPs shall contain some information concerning the Publication they belong to, date, edition / amendment etc., which shall not be User modifiable.

2.2 CONFIGURATION CONTROL OF CLASS X AND XP IETPS

There is a single site (the server) managed by the Company which provides the IETP (the Company) where the latest official version of the Publications is made available to the user; this can be viewed with the applicable software (the Client with dedicated SW or commercial browser).

One or more persons (the Administrators) are responsible for managing and monitoring the distribution Server for this site.

The administrators contribute to preparing the IETP User manual.

The manual covers all aspects concerning the methods of processing and viewing the data contained in the IETPs, via network.

In the same way, on the User side there shall be an appropriate control policy which includes an Administrator with the task of supervising installations and Users.

The IETPs can only be viewed via the Client (the Client with dedicated SW or commercial browser).

The IETPs shall be protected in order to avoid modification of the data stored on the Server. It is the Company's responsibility to ensure the integrity of the data stored on the server and protect them against unauthorized modification.

The Server shall contain an on-line help menu listing complete procedures.

This will include step-by-step instructions for correct Client installation, when required.

If the Client can be installed on different operating systems, a procedure shall be prepared for each individual operating system.

Users shall be notified automatically of the presence of new modifications on the site via on-screen notifications (e.g.; pop-ups). In addition, any modifications shall be indicated by the Client (the Client with dedicated SW or commercial browser), as described later in this regulation.

The Client (the Client with dedicated SW) downloaded from the server shall only allow access to data via authentication.

The Client (the Client with dedicated SW or commercial browser) shall not allow any modification to be made to the individual DMs / IETPs stored on the Server. Any addition of bookmarks or notes shall be managed via separate files either saved locally or on the server.

The Client (the Client with dedicated SW or commercial browser) shall:

➢ Highlight, at the start of each connection, the presence of an entire new edition or updates to the IETP being viewed, via notifications on screen via pop-up, with respect to the last access made by the User;

➢ Place identifying data on each hardcopy printout requested by the User, in compliance with AER.P-170 regulation.

The individual DMs / IETPs shall contain some information concerning the Publication they belong to, date, edition / revision etc., which shall not be User modifiable.

2.3 SECURITY OF TRANSMITTED DATA

The first connection shall occur using a Username and Password, earlier provided in a secured way.

The User shall then set a personalized Password for the next connection.

Based on the assessment performed by Armed Forces / State Corps departments, each User shall be only allowed to access the data for which the access has been previously authorized by Armed Forces / State Corps departments.

This access can be either extended or changed only as per jointly authorization by the system Administrators.

The Server shall periodically force the password change according to a time schedule to be defined.

The Server-side network infrastructure shall include a Hardware Firewall in order to protect the data contained from unwanted access and avoid communication port saturation; redundancy shall be provided to guarantee continued availability of the information over the network.

The data shall backed up to a location that is isolated from the communications network.

The sent data shall be encrypted via a Hardware and/or Software procedure to be evaluated on the basis of the classification level of the data to be sent, both for individual DMs or entire IETPs.

If the document is classified, a cryptographic algorithm with a minimum 256 bit key size is required (e.g. Advanced Encryption Standard – AES).

The sent data shall be encapsulated in packets, accompanied by information such as to guarantee the integrity and original nature of the data itself during transit from the Server to the Client.

Two simultaneous connections shall not be allowed for the same User.

2.4 DATA TRANSMISSION NETWORK

The Data Transmission Network shall be chosen and sized in such a way as to guarantee sufficient data transmission speeds for the expected reaction times of the system, the quantity of data to be transferred and the number of Users.

In the event that public data networks (Internet) and http protocol are used, access to the portal and the publication data shall require an authentication process (e.g. username, password), which shall be performed via the use of cryptographic protocols (SSL/TLS or successive evolutions) which provide secure communications (HTTPS).

Except where the data are Non Classified, the authentication process shall be further reinforced (e.g. through handshaking of a digital certificate uniquely issued by the company's certification authority to the user, by means of an auto-enrolment procedure which authorizes the user to access the service exclusively from the client that he/she used to submit the authorization request).

If required, sufficient redundancy shall be provided in order to prevent interruptions of a communication line.

Radio or satellite links should be used where necessary.

2.5 DATA WITH SECURITY LEVEL ABOVE RESTRICTED

All data with security classification of "Confidential" or above shall be made available on the appropriate existing media (e.g. CD-ROM / DVD-ROM), i.a.w. the regulations established by the technical standards listed in section 1.2.

2.6 DAAA AREA FOR EVALUATION OF TECHNICAL MANUALS

If contractually required, the website shall provide an area accessible only to users authorised by DAAA to carry out the evaluation of the sample copy / draft sample copy of the Technical Publications and for the management of any related documentation.

2.7 TECHNICAL MANUAL OF THE PORTAL FOR REMOTE VIEWING OF IETPS

On the basis of the requirements defined in this regulation, the Company providing the IETPs on a portal for remote access shall prepare a Technical Manual i.a.w. the current edition of AER(EP).0-0-2.

The identification code of the Technical Manual shall have:

- Class code:
  32 (manuals for ground equipment, standard and special)

- Subject or material code:
  PORTAL DRS/MDS

- Publication Code:
  -1

E.G.: AER(EP).32-SDR PORTAL/MDS-1 Description and instructions for use of the portal for remote viewing of IETPs of the MDS aircraft.