DECIZIA
DIRECTORULUI GENERAL AL
AUTORITĂŢII AERONAUTICE CIVILE ROMÂNE

Nr.D729/2025

În temeiul prevederilor Hotărârii Guvernului nr. 405/1993 privind înființarea Autorității Aeronautice Civile Române, cu modificările și completările ulterioare,

Pentru îndeplinirea atribuțiilor ce revin Autorității Aeronautice Civile Române în calitatea sa de autoritate competentă responsabilă cu coordonarea și monitorizarea aplicării standardelor de bază comune stabilite de Regulamentul (CE) nr. 300/2008,

Având în vedere prevederile Ordinul ministrului transporturilor nr. 1547/2013 privind delegarea de competență și desemnarea Regiei Autonome "Autoritatea Aeronautică Civilă Română" ca organism tehnic specializat pentru exercitarea unor atribuții ce revin autorității competente în domeniul securității aviației civile, la nivel naţional, precum şi pentru stabilirea unor măsuri necesare realizării acestei delegări de competenţe,

În baza prevederilor Hotărârii Consiliului de Administrație nr. 1/09.01.2023 privind desemnarea Directorului General, precum şi competențelor stabilite prin Contractul de mandat nr. 760/09.01.2023 încheiat între R.A. Autoritatea Aeronautică Civilă Română prin Consiliul de Administrație și domnul Nicolae Stoica, în calitate de Director General,

În temeiul prevederilor punctelor 1.3.8, 6.3.3 și 10.2.2 din Programul Național de Pregătire în domeniul securității aviației civile, aprobat prin Ordinul Ministrului Transporturilor și Infrastructurii nr. 1145 din 31 iulie 2025 - PNPSAC,

Directorul General al Autorității Aeronautice Civile Române,

DECIDE:

Art. 1 - Se aprobă *Instrucțiunile privind modalitățile de implementare a prevederilor Programul Național de Pregătire în domeniul securității aviației civile, cu privire la pregătirea în domeniul securității cibernetice* prevăzute în anexa la prezenta.

Art. 2 - Instrucțiunile prevăzute la art. 1 sunt destinate operatorilor și entităților menționate la punctul 1.3.2, literele a), b), e), g), h) (cu excepția transportatorilor rutieri) și k) din PNPSAC și vor fi avute în vedere la asigurarea pregătirii specifice.

Art. 3 - Structura Securitate Aeronautică asigură comunicarea prezentei decizii tuturor părților interesate.

Art. 4 – Începând cu data prezentei decizii, Decizia directorului general al Autorităţii Aeronautice Civile Române pentru aprobarea *Instrucțiunilor privind modalitățile de implementare a prevederilor Capitolului 10.3 din Programul Național de Pregătire în domeniul Securității Aviației Civile* nr. D725/2024, își încetează aplicabilitatea.

Art. 5 – Dovezile de pregătire emise în baza prevederilor Deciziei directorului general al Autorităţii Aeronautice Civile Române nr. D725/2024 își păstrează valabilitatea timp de 5 ani de la data pregătirii.

(E-signed)
DIRECTOR GENERAL
Nicolae STOICA

Anexa la Decizia Directorului General
al AACR nr. 729/2025

Instrucțiunile privind modalitățile de implementare a prevederilor Programul Național de Pregătire în domeniul securității aviației civile, cu privire la pregătirea în domeniul securității cibernetice

PARTEA A
GENERALITĂȚI

1. Scop

Prezentele instrucțiuni stabilesc modalitatea de implementare a prevederilor Programului Național de Pregătire în domeniul Securității Aviației Civile, aprobat prin OMTI nr. 1145 / 2025 (denumit în continuare ”Program”), privind:

1.1. Pregătirea personalului responsabil cu aplicarea măsurilor de securitate din cadrul operatorilor și entităților prevăzute la punctul 1.3.2 literele a), b), e), g), h) (cu excepția transportatorilor rutieri) și k) din Program și care are acces la datele și sistemele de tehnologie a informației și comunicațiilor critice (utilizatori), așa după cum au fost acestea identificate de Programul de Securitate al entității respective, în aplicare prevederilor punctelor 1.7.1 – 1.7.3 din Anexa la Regulamentul (UE) 2015/1998;

1.2. Pregătirea persoanelor care dețin drepturi de administrator și/sau au acces nesupravegheat și nelimitat la datele și sistemele de tehnologie a informației și comunicațiilor critice, astfel cum acestea sunt identificate prin Programul de Securitate al operatorilor și entităților menționate la punctul 1.1, în aplicare prevederilor punctelor 1.7.1 – 1.7.3 din Anexa la Regulamentul (UE) 2015/1998.
Prin acces nesupravegheat se înțelege că o persoană, cu drepturi de acces care îi permit să facă modificări în timpul conectării la un sistem / date critice, nu este sub supraveghere sau monitorizată în mod continuu pentru a fi prevenită / împiedicată o acțiune ilicită, sau, în cazul în care persoana săvârșește acțiunea ilicită, pentru a fi detectată imediat și sistemul / datele critice să fie recuperate.
Prin acces nelimitat se înțelege că drepturile de acces nu sunt limitate în cadrul arhitecturii unui sistem / date critice (care acordă acces activ și posibilități de interferare) sau, în cazul în care drepturile sunt limitate, zonele pentru care persoana deține acces deplin cuprind zone în care acesta poate provoca daune sistemelor / datelor de securitate.

2. Documente de referință

- Regulamentul de punere în aplicare (UE) 2015/1998 al Comisiei din 5 noiembrie 2015 de stabilire a măsurilor detaliate de implementare a standardelor de bază comune în domeniul securității aviației, cu modificările și completările ulterioare,
- Decizia C(2015)8005 a Comisiei din 16.11.2015 de stabilire a măsurilor detaliate de implementare a standardelor de bază comune privind securitatea aviației care conțin informațiile menționate la articolul 18 litera a) din Regulamentul (CE) nr. 300/2008, cu modificările și completările ulterioare, în special Decizia C(2017) 3030 a Comisiei;
- Ordinul Ministrului Transporturilor și Infrastructurii nr. 1145 din 31 iulie 2025 pentru aprobarea Programului Național de Pregătire în domeniul Securității Aviației Civile.

PARTEA B
CERINȚE DE PREGĂTIRE

I. Pregătirea ”utilizatorilor”

1. Pregătirea utilizatorilor se realizează intern, prin intermediul unei persoane autorizate.

2. Prin persoană autorizată se înțelege:
- managerul de securitate definit la Capitolul 3, punctul 10, din Program, și/sau
- o persoană care deține drepturi de administrator și/sau au acces nesupravegheat și nelimitat la datele și sistemele de tehnologie a informației și comunicațiilor critice, menționată la capitolul 10 din Program.

3. Persoanele autorizate se stabilesc prin decizie / dispoziție / desemnare formală a directorului general / administratorului operatorilor și entităților prevăzute la punctul 1.1. Prin excepție, persoanele sunt considerate autorizate dacă sunt menționate explicit în programul de securitate și/sau programul de pregătire, ca asigurând pregătirea utilizatorilor.

4. După desemnare și înainte de a desfășura orice formă de pregătire pentru utilizatori, persoanele autorizate vor parcurge un curs de pregătire (”train the trainers”), gratuit, organizat de către Autoritatea Aeronautică Civilă Română - AACR și susținut de către Directoratul Național de Securitate Cibernetică - DNSC.

5.1 Durata pregătirii menționate la punctul 4 este de cel mult o zi (8 ore) și se va desfășura în format fizic. Prin excepție, în cazuri întemeiate, AACR, în colaborare cu DNSC, poate decide ca pregătirea menționată la punctul 4 să se desfășoare online / în sistem hibrid.

5.2 Sesiunile de pregătire pentru persoanele autorizate se organizează în vederea autorizării respectiv a reautorizării, la intervale de maximum 5 ani. În situația în care este necesar, AACR în colaborare cu DNSC pot organiza sesiuni speciale de pregătire în cazurile în care se constată necesitatea unei actualizări de urgență a instrucțiunilor (ex. urmare a unor incidente cu impact semnificativ sau apariției unor amenințări severe care impun măsuri de urgență).

5.3. Operatorii și entitățile prevăzute la punctul 1.1 vor transmite AACR solicitarea de înscriere la următoarea sesiune de pregătire a persoanelor autorizate. Solicitarea va cuprinde dovada desemnării și datele de contact (telefon și e-mail) ale persoanelor autorizate.

5.4. Persoanele autorizate, acceptate pentru a participa la următoarea sesiune de pregătire organizată de către AACR și susținută de către DNSC, vor fi notificate de către AACR, prin e-mail, cu cel puțin 15 zile înainte de data organizării acesteia. Directorii generali / administratorii operatorilor și entităților prevăzute la punctul 1.1 vor asigura participarea persoanelor pe care le-au autorizat la data, ora și locația stabilite pentru sesiunea de pregătire.

6. În cadrul pregătirii interne pe care o vor asigura, persoanele autorizate vor respecta specificațiile prevăzute în Anexa nr. 1 și conținutul pregătirii din Anexa nr. 2.

7. Suplimentar cerinței de la punctul 6, în procesul de personalizare a pregătirii pe specificul entității, persoanele autorizate vor asigura adaptarea conținutului pregătirii utilizatorilor la datele și sistemele de tehnologie a informației și comunicațiilor critice identificate prin Programul de Securitate al entității respective, precum și la specificul activităților așa cum sunt ele organizate intern, decurg din organigramă, regulamentul de organizare și funcționare sau alte regulamente interne, ori din deciziile conducerii privind atribuțiile persoanelor și ale departamentelor, lanțul decizional intern, fluxul de activități specifice și modul stabilit de îndeplinire a sarcinilor, în aplicarea prevederilor punctelor 1.7.1 – 1.7.3 din Anexa la Regulamentul (UE) 2015/1998.

8. Se recomandă ca la elaborarea conținutului de curs, persoanele autorizate să aibă în vedere Metodologia - *Awareness Raising (AR) in a box* – dezvoltată de Agenția pentru Securitate Cibernetică a Uniunii Europene (ENISA). Pentru aceasta, în cadrul sesiunii de pregătire susținute de către DNSC va fi inclus un capitol dedicat utilizării Metodologiei - *Awareness Raising (AR) in a box*.

9. Înainte de a desfășura orice formă de pregătire pentru utilizatori, persoanele autorizate au obligația de a parcurge cursul interactiv AR-in-a-Box, disponibil prin EU Academy la următoarea adresă: https://academy.europa.eu/courses/ar-in-a-box-build-your-own-cyber-awareness-program.
Pagina oficială a AR-in-a-Box este disponibilă la următoarea adresă: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box.

II. Pregătirea persoanelor care dețin drepturi de administrator sau au acces nesupravegheat și nelimitat la datele și sistemele de tehnologie a informației și comunicațiilor critice

Persoanele care dețin drepturi de administrator sau au acces nesupravegheat și nelimitat la datele și sistemele de tehnologie a informației și comunicațiilor critice trebuie să facă dovada că dețin:

- o certificare în domeniul ITC și securității cibernetice, recunoscută pe plan național sau internațional. Lista certificărilor se regăsește în Anexa nr. 3*

** Lista va fi completată/actualizată, permanent, în baza evaluării realizate de DNSC, în calitate de autoritate competentă la nivel național.*

III. Alte cerințe de pregătire

Atât utilizatorii, cât și persoanele care dețin drepturi de administrator sau au acces nesupravegheat și nelimitat la datele și sistemele de tehnologie a informației și comunicațiilor critice, trebuie să fi trecut cu succes cel puțin printr-o pregătire de conștientizare în materie de securitate a aviației civile (Modulul 1 la Program) sau printr-o pregătire de bază în securitatea aviației civile (Modulul 26 la Program), înainte să li se permită preluarea sarcinilor de serviciu.

Anexa nr. 1
la Instrucțiunile privind modalitățile de implementare a prevederilor Programul Național de Pregătire în domeniul securității aviației civile (PNPSAC 2025)

Categoria de personal:	**Persoanele care au acces la datele și sistemele de tehnologie a informației și comunicațiilor critice - utilizatori (punctul 1 lit. x) din Anexa nr. 1)**
Conținutul pregătirii:	Modulul 27
Obiectivele învățării:	Obiectivul principal este de a se asigura că utilizatorii înțeleg importanța măsurilor de securitate cibernetică în securitatea aviației civile și primesc o pregătire corespunzătoare și specifică funcției ocupate, proporțională cu rolul și responsabilitățile sale, inclusiv să fie informați în legătură cu riscurile relevante atunci când funcția impune acest lucru.
Competențe / Cunoștințe / Deprinderi	Modulul 27 ▪ înțelegerea terminologiei de bază aplicabile în domeniul securității cibernetice, cum ar fi: amenințări, vulnerabilități, riscuri; ▪ înțelegerea principiilor de securitate cibernetică: confidențialitate, integritate, disponibilitate; ▪ cunoașterea tipurilor principale de amenințări și atacuri; ▪ cunoașterea principalelor măsuri de prevenire a incidentelor din domeniul securității cibernetice din perspectiva unui utilizator; ▪ înțelegerea măsurilor de protecție aplicabile în mediul digital; ▪ cunoașterea elementelor de bază privind asigurarea unui răspuns la amenințări și incidente; ▪ înțelegerea cadrului legal aplicabil în domeniul securității cibernetice, inclusiv Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, aprobată cu modificări și completări prin Legea nr. 124/2025, precum și actele normative elaborate în vederea aplicării acesteia.
Durata minimă:	Cursul trebuie să aibă o durată de minim 8 ore
Evaluare:	Fiecărei persoane care beneficiază de pregătire de conștientizare în materie de securitate cibernetică în securitatea aviației civile trebuie să i se solicite să demonstreze înțelegerea tuturor aspectelor sus menționate înainte de a avea acces la date și sisteme de tehnologie a informației și comunicații critice. Cunoștințele trebuie să fie

	verificate prin intermediul unui test scris al cărui punctaj minim de promovare este de 75%..
Pregătirea inițială:	Pregătirea inițială trebuie să fie efectuată înainte ca personalului să i se permită preluarea sarcinilor de serviciu.
Pregătirea periodică:	Pregătirea periodică trebuie să se desfășoare la intervale de cel mult 5 ani pentru a se asigura că menținerea și dobândirea competențelor sunt corelate cu evoluțiile din domeniul securității cibernetice din securitatea aviației civile. Pregătirea periodică trebuie să conțină cel puțin componentele principale ale modulelor relevante, aşa cum acestea sunt descrise în prezentul document și va pune accentul pe modificările cerințelor şi practicilor apărute în perioada scursă de la pregătirea anterioară. Pregătirea periodică va avea o durată de minim 4 ore. Personalul trebuie informat, prin notificări periodice, cu privire la schimbările survenite în toate aspectele privind cunoștințele de securitate și abilitățile ce îi sunt necesare în îndeplinirea sarcinilor de serviciu.
Categoria de personal:	**Persoanele care au drepturi de administrator și/sau au acces nesupravegheat și nelimitat la datele și sistemele de tehnologie a informației și comunicațiilor critice - administratori (punctul 1 lit. y) din Anexa nr. 1)**
Conținutul pregătirii:	Modulul 28
Obiectivele învățării:	Obiectivul principal este de a se asigura că administratorii au și își mențin competențele și aptitudinile necesare pentru îndeplinirea sarcinilor desemnate la un nivel adecvat. Administratorii trebuie să fie informați cu privire la riscurile cibernetice relevante, pe baza principiului necesității de a cunoaște.
Competențe / Cunoștințe / Deprinderi	Modulul 28 O certificare în domeniul ITC și securității cibernetice, recunoscută pe plan național sau internațional. Lista certificărilor se regăsește în Anexa nr. 3
Durata minimă:	Durata pregătirii specifice este stabilită conform cerințelor pentru fiecare certificare menționată în Anexa nr. 3.
Evaluare:	Evaluarea pregătirii specifice este stabilită conform cerințelor pentru fiecare certificare menționată în Anexa nr. 3
Pregătirea inițială:	Administratorii trebuie să fie certificați conform cerințelor prezentului document înainte să aibă acces la date și sisteme de tehnologie a informației și comunicații critice.

Pregătirea periodică: Conform cerințelor pentru păstrarea competențelor ca urmare a obținerii uneia din certificările menționate în Anexa nr. 3

Administratorii trebuie informați, prin notificări periodice, cu privire la schimbările survenite în toate aspectele privind cunoștințele de securitate cibernetică și abilitățile care le sunt necesare pentru îndeplinirea sarcinilor desemnate.

Anexa nr. 2
la Instrucțiunile privind modalitățile de implementare a prevederilor Programul Național de Pregătire în domeniul securității aviației civile, cu privire la pregătirea în domeniul securității cibernetice

MODULUL 27 – PREGĂTIRE DE CONȘTIENTIZARE ÎN SECURITATE CIBERNETICĂ

Aspecte de învățat:

Cunoașterea terminologiei de bază în domeniul securității cibernetice:
- Amenințări;
- Vulnerabilități;
- Riscuri;
- Incidente.

Înțelegerea principiilor fundamentale aplicabile în domeniul securității cibernetice:
- Principiul confidențialității;
- Principiul integrității;
- Principiul disponibilității;
- Principiul autenticității;
- Principiul nonrepudierii.

Cunoașterea tipurilor de amenințări și atacuri cibernetice:
- Malware;
- Atacuri de tip phishing și inginerie socială;
- Atacuri de rețea (DoS/DDoS, MITM, spoofing);
- Exploatarea vulnerabilităților software.

Înțelegerea noțiunilor de bază privind măsurile de gestionare a riscurilor:
- Identificarea și inventarierea activelor relevante;
- Identificarea amenințărilor și vulnerabilităților asociate;
- Evaluarea riscurilor (probabilitate și impact);
- Măsuri de reducere a riscurilor: prevenire, transfer, acceptare, atenuare.

Cunoașterea elementelor de baza privind asigurarea unui răspuns la amenințări și incidente:
- Detectarea și clasificarea incidentelor;
- Limitarea efectelor și izolarea sistemelor afectate;
- Eliminarea cauzei și remedierea vulnerabilităților;
- Restaurarea funcționalității, implementarea unor măsuri de back-up.

Înțelegerea cadrului legal aplicabil securității cibernetice:
- Cunoașterea termenilor și a noțiunilor privind securitatea cibernetică aplicabile la nivelul entităților esențiale și importante în conformitate cu legislația în vigoare în domeniul securității cibernetice de la nivelul României și UE;
- Autoritatea competentă și obligațiile entităților esențiale și importante conform actelor normative aplicabile în domeniul securității cibernetice.

Anexa nr. 3
la Instrucțiunile privind modalitățile de implementare a prevederilor Programul Național de Pregătire în domeniul securității aviației civile, cu privire la pregătirea în domeniul securității cibernetice

LISTA CERTIFICĂRILOR PROFESIONALE[1]

#	Certificare		
1.	C)PEH	-	Certified Professional Ethical Hacker
2.	C)PTC	-	Certified Penetration Testing Consultant
3.	C)PTE	-	Certified Penetration Testing Engineer
4.	CASP +	-	CompTIA Advanced Security Practitioner
5.	CEH	-	EC-Council Certified Ethical Hacker
6.	CEPT	-	IACRB Certified Expert Penetration Tester
7.	CGEIT	-	Certified in the Governance of Enterprise IT
8.	CHA	-	Certified Hacker Analyst
9.	CHAT	-	Certified Hacker Analyst Trainer
10.	CISA	-	Certified Information Systems Auditor
11.	CISM	-	Certified Information Security Manager
12.	CISSP	-	Certified Information Systems Security Professional
13.	CMWAPT	-	IACRB Certified Mobile and Web Application Penetration Tester
14.	COBIT5	-	COBIT 5 Certification
15.	CPT	-	IACRB Certified Penetration Tester
16.	CRISC	-	Certified in Risk and Information Systems Control
17.	CTA	-	OSSTMM Certified Trust Analyst
18.	CySA +	-	CompTIA Cybersecurity Analyst
19.	ECSA	-	EC-Council / Certified Security Analyst
20.	GCIP	-	GIAC Critical Infrastructure Protection
21.	GIAC	-	GSNA Systems and Network Auditors
22.	GIAC	-	GCCC Critical Controls Certification
23.	GICSP	-	GIAC Global Industrial Cyber Security Professional
24.	GPEN	-	GIAC Certified Penetration Tester
25.	GRID	-	GIAC Response and Industrial Defense
26.	GWAPT	-	GIAC Web Application
27.	GXPN	-	GIAC Exploit Researcher and Advanced Penetration Tester
28.	LPT	-	EC-Council / Licensed Penetration Tester
29.	OPSA	-	OSSTMM Professional Security Analyst

30.	OPSE	-	OSSTMM Professional Security Expert
31.	OPST	-	OSSTMM Professional Security Tester Accredited Certification
32.	OSCE	-	Offensive Security Certified Expert
33.	OSCP	-	Offensive Security Certified Professional
34.	OSWE	-	Offensive Security Web Expert
35.	OSWP	-	Offensive Security Wireless Professional
36.	OWSE	-	OSSTMM Wireless Security Expert
37.	PenTest+	-	CompTIA PenTest+

[1] *Lista va fi completată/actualizată, permanent, în baza evaluării realizate de DNSC, în calitate de autoritate competentă la nivel național..*