AUTORITATEA ELECTORALĂ PERMANENTĂ

PROCEDURĂ DE SISTEM
PROCEDURĂ FORMALIZATĂ PRIVIND ACCESUL ÎN SISTEMUL INFORMATIC AL AEP ȘI GESTIONAREA RESURSELOR IT PUSE LA DISPOZIȚIA UTILIZATORILOR

PS.05

APROB,
PREȘEDINTE
[redacted]

AVIZAT,
PREŞEDINTELE COMISIEI DE MONITORIZARE
A AUTORITĂȚII ELECTORALE PERMANENTE
[redacted]

VERIFICAT,
DIRECTOR GENERAL DIPE
[redacted]

VERIFICAT,
DIRECTOR DEEI
[redacted]

VERIFICAT,
DIRECTOR DDSA
[redacted]

ELABORAT,
CONSILIER PARLAMENTAR
[redacted]

Ediția: 1
Revizia: 0
Data: 22.01.2025

Cuprins

1. Scopul procedurii

- Acordarea accesului și autentificarea utilizatorului în SIAEP
- Instalarea și configurarea programelor de calculator
- Evidența programelor instalate

2. Domeniul de aplicare a procedurii:

Procedura se aplică de către toți angajații AEP.

3. Documente de referință (reglementări) aplicabile activității procedurale:

a. Hotărârea Nr. 4 / 2020 a Birourilor permanente ale Camerei Deputaților și Senatului, privind aprobarea privind aprobarea Regulamentului de organizare și funcționare a Autorității Electorale Permanente;

b. Regulamentului intern al Autorității Electorale Permanente aprobat prin Ordinul nr. 851/15.09.2022

c. Ordinele emise de președintele Autorității Electorale Permanente;

d. Ordinul Secretarului General al Guvernului nr. 400 din 12 iunie 2015 pentru aprobarea Codului controlului intern managerial al entităților publice, cu modificările și completările ulterioare;

e. Ordonanța Guvernului nr. 119/1999 privind controlul intern/managerial și controlul financiar preventiv, aprobată prin Legea nr. 301/2002, republicată, cu modificările și completările ulterioare;

f. Standardele de management/control managerial;

g. Fișa postului;

h. Norme PSI-SU și SSM;

4. Definiții și abrevieri ale termenilor utilizați în procedură:

4.1. Definiții ale termenilor:

SIAEP – Totalitatea echipamentelor, programelor și procedurilor IT&C se constituie în Sistemul Informatic al AEP (SIAEP).

Procedură operațională - prezentarea formalizată, în scris, a tuturor pașilor ce trebuie urmați, a metodelor de lucru stabilite și a regulilor de aplicat în vederea realizării activității, cu privire al aspectul procesual

Ediție a unei proceduri operaționale - Forma inițială sau actualizată, după caz, a unei proceduri operaționale, aprobată și difuzată

Revizia în cadrul unei ediții - Acțiunile de modificare, adăugare, suprimare sau altele asemenea, după caz, a uneia sau mai multor componente ale unei ediții a procedurii operaționale, acțiuni care au fost aprobate și difuzate

IT&C – Abreviere pentru tehnologia informațiilor și comunicații

Intranet – Abreviere pentru o rețea privată TCP/IP care asigură utilizatorilor dintr-o rețea locală servicii de tip internet, cum ar fi site-urile web

AD - Active Domain, platformă de administrare a utilizatorilor și a drepturilor aferente ale acestora pe calculatoarele de serviciu

Browser – program folosit pentru navigarea pe internet

Cod malițios - Este, în general, descris ca un fișier sau tip de program care interferează cu funcționarea normală a sistemului de operare. Poate fi folosit pentru preluarea controlului resurselor unui sistem informatic, pentru furtul de date confidențiale ori pentru instalarea de aplicații dăunătoare (malware). În literatura de specialitate, codul malițios este menționat ca virus, vierme sau Cal Troian.

Malware – Cod răuvoitor – orice program de calculator sau cod care a fost creat (dezvoltat) cu scopul de a „invada" sisteme de calcul și de a cauza probleme.

Troian - Calul Troian este o aplicație de backdoor, disimulat într-un program legitim care, odată lansat execuție, instalează pe computerul țintă, o încărcătură dăunătoare (ex. viruși, keylogger etc.). Este un program de calculator care pare a fi benefic sau inofensiv, însă are și o funcție ascunsă și posibil malițioasă care se sustrage mecanismelor de securitate. Un „Înregistrator de taste" care înregistrează tastările victimelor și le trimite unui atacator, sau „computerele zombie" controlate de la distanță, sunt exemple de prejudicii care pot fi aduse de caii troieni.

Infecții electronice - Adesea denumite „viruși", aceste programe și coduri rău intenționate vă infectează negativ computerul și vă compromit confidențialitatea. Pe lângă virușii tradiționali, alte tipuri obișnuiți includ viermi și cai troieni. Aceștia lucrează uneori în tandem pentru a realiza prejudiciul maxim.

4.2. Abrevieri ale termenilor:

Nr. crt.	Abrevierea	Termenul abreviat
1.	PO	Procedură operațională
2.	E	Elaborare
3.	V	Verificare
4.	Av	Avizare
5.	A	Aprobare
6.	Ap	Aplicare
7.	Ah	Arhivare
8.	AEP	Autoritatea Electorală Permanentă
9.	DIPE	Departamentul Informatizarea Proceselor Electorale
10.	DEEI	Direcția evidențe electorale informatizate
11.	DDSA	Direcția dezvoltare software și aplicații
12.	SIAEP	Sistemul Informatic al AEP

13.	CM	Comisia de monitorizare
14.	LAN	Local Area Network, rețeaua internă a AEP
15.	AD	Active Domain
16.	OS	Operating System, sistem de operare al unui calculator

5. Descrierea procesului (Mod de lucru):

5.1. Generalități

Componente ale Sistemului Informatic al AEP:

- Echipamente IT&C (enumerare): calculatoare personale și perifericele conectate la acestea, rețeaua internă care leagă aceste calculatoare între ele și cu alte periferice de rețea, servere, storage, routere și switch-uri, legătura cu exteriorul (asigurată prin legarea rețelei interne de rețeaua de Internet, sistemul de e-mail și pagina web a instituției). Echipamente IT&C locație: sediul central al AEP și sediile direcțiilor instituției
- Programe IT: totalitatea programelor instalate în echipamentele IT&C și care administrează și organizează aceste echipamente și rețelele care le conectează. Programe IT&C locație: sediul central al AEP și sediile direcțiilor instituției.

SIAEP este gestionat de personalul DIPE din cadrul AEP. Anumite servicii specifice pot fi externalizate. Gestionarea se face din locațiile AEP. În cazuri justificate, anumite activități pot fi desfășurate de la distanță prin intermediul unor conexiuni securizate cu aprobarea șefului de compartiment.

Personalul DIPE reprezintă partea de administrare a SIAEP, iar ceilalți angajați AEP constituie utilizatorii SIAEP.

În scopul asigurării securității informațiilor și datelor AEP, personalul autorizat poate revizui sau utiliza orice informație stocată pe SIAEP sau transportată prin SIAEP în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor pe calculatoarele de serviciu (de exemplu: paginile web vizitate).

Utilizatorii trebuie să raporteze orice vulnerabilitate a sistemului de securitate al SIAEP, orice incident de posibilă întrebuințare greșită SIAEP.

Niciun utilizator al SIAEP nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemelor ce compun resursele SIAEP.

În cadrul SIAEP, se utilizează platforme hardware, sisteme de operare și aplicații informatice. Caracteristicile de securitate ale acestor sisteme sunt activate implicit și previn o multitudine de atacuri cibernetice des întâlnite. În cadrul AEP se utilizează sisteme de operare pe 64 de biți deoarece acestea solicită eforturi mai mari din partea unui atacator care încearcă să capete controlul unui computer.

Parte a SIAEP, soluțiile de securitate instalate oferă cel puțin protecție de tip antivirus, antimalware, antispam și antiphishing, atât la nivelul calculatoarelor de serviciu, cât și la nivelul serverelor fizice și virtuale. O altă caracteristică a acestor soluții de securitate este verificarea site-urilor accesate, având un istoric al reputației domeniilor web care au avut vreodată un rol în răspândirea de malware.

DIPE utilizează mecanisme privind administrarea adecvată a accesului la sistemele/programele informatice importante gestionate de către aceștia:

- Principalele sisteme/programe informatice sunt utilizate numai pe bază de identificator unic, parolă personală secretă și drepturi de acces.

- Controlul accesului la aplicaţii este configurat astfel încât să minimalizeze riscurile cu privire la securitatea informaţiei şi să permită desfăşurarea în bune condiţii a activităţilor desfăşurate.
- Utilizatorii au acces numai la comenzile, funcţiile din sistem, datele şi informaţiile pe care au dreptul să le folosească.
- Accesul la anumite date considerate cu caracter personal, în conformitate cu prevederile legale, este permis numai angajaţilor care au nevoie de aceste informaţii în îndeplinirea sarcinilor ce le revin.
- Pentru accesarea sistemul de operare se va utiliza o parolă de utilizator (user) cu drepturi suficiente pentru îndeplinirea obligaţiilor.
- Se interzice divulgarea datelor de autentificare în SIAEP sau utilizarea unui cont de către alt utilizator decât cel care nu deţine acel cont.
- Interzicerea folosirii de către utilizatori a programelor software care provin din surse nelegitime;

Se utilizează doar parole complexe. Ca regulă generală, toate parolele asociate cu orice cont de utilizator SIAEP trebuie să aibă cel puţin 8 caractere, trebuie să includă minim un caracter special, o cifră, litere mici şi minim o literă mare.

În vederea utilizării conturilor de e-mail, pentru a reduce riscurile asociate utilizării acestui serviciu, se va ţine seamă de recomandările formulate în Procedura operaţională privind utilizarea serviciului de poştă electronică.

Periodic sunt efectuate operaţiuni de optimizare, diagnosticare şi verificare care asigură rularea aplicaţiilor în cele mai bune condiţii. Mentenanţa resurselor informatice, a mediilor de comunicaţii şi a echipamentelor IT&C şi de suport se realizează prin intermediul DIPE. Programele de întreţinere care vor fi rulate vor îndeplini următoarele funcţii: actualizarea sistemului de operare, actualizarea şi scanarea antivirus, actualizarea punctelor de *system restore* şi asigurarea back-up-ului pentru fişierele de lucru ale utilizatorului.

În cazul utilizării SIAEP de către persoane din afara AEP, accesul este controlat, printr-un cont cu facilităţi de acces restrânse (*cont guest*).

Reguli de securitate pentru utilizatorii SIAEP cu privire la:

a. Browsere - acestea permit accesarea şi vizualizarea site-urilor, navigarea prin link-uri, descărcarea de fişiere de pe internet etc. Pentru a reduce riscurile legate de navigarea pe internet, utilizatorii SIAEP nu trebuie să acceseze link-uri care sunt marcate drept periculoase de către soluţia de securitate instalată pe sistem, sau de către browser-ul de internet. La primirea oricărui mesaj de atenţionare în timpul navigării spre o pagină marcată ca potenţial periculoasă, utilizatorii nu trebuie să o acceseze

b. Conturile de e-mail:

- Setarea unor mesaje de genul "out-of-office" pentru contul personal de e-mail nu este recomandată, fiind o sursă preţioasă de informaţii pentru spammeri şi confirmând faptul că este o adresă de e-mail validă;
- E-mailurile nesolicitate, care conţin ataşamente sau link-uri, trebuie tratate ca suspecte. Dacă identitatea celui care a trimis respectivul e-mail nu poate fi verificată, sfatul este de a şterge acel e-mail fără a-l deschide pentru a-i vedea conţinutul. Nu răspundeţi la e-mailuri care vă solicită date cu caracter personal. Orice entitate cu care relaţionaţi prin intermediul unor aplicaţii web ar trebui deja să aibă aceste informaţii. În cazul e-mailurilor care conţin link-uri, nu navigaţi direct către acel link. Puteţi copia acel link şi să îl căutaţi de exemplu pe Google. Dacă este absolut

necesară deschiderea unui atașament, se recomandă ca acesta să fie descărcat și scanat cu soluția antivirus instalată pe calculator;

- Nu se accesează mesajele marcate de către programul client de e-mail sau de către antivirus ca spam;
- Nu accesați mesaje privind cardul de credit sau invitații diverse care provin din partea unor surse necunoscute.
- Nu trimiteți niciodată parolele dumneavoastră de cont prin e-mail sau prin atașamente. Nici un furnizor de servicii nu solicită astfel de informații;

c. Utilizarea porturilor USB, a unităților CD/CD-writer sau altor dispozitive de intrare/ieșire se va face doar pentru transferul datelor în interes de serviciu.

- Este interzisă introducerea de software malițios prin intermediul acestor dispozitive

5.2. Modul de lucru

I. Compartimentul AEP în care desfășoară activitatea un nou angajat completează nota eliberare mijloace fixe sau obiecte de inventar din magazie.

II. După primirea de către DIPE a notei aprobate și a calculatorului, persoana responsabilă din cadrul DIPE instalează sistemul de operare și înrolează noul utilizator în Active Domain-ul (AD) AEP. Astfel, pentru fiecare angajat este creat un cont de utilizator cu nume și parolă, necesar pentru autentificarea în sistemul de operare al calculatorului de serviciu.

III. Parola de acces în AD se schimbă obligatoriu la fiecare 6 luni de către fiecare angajat al AEP printr-o notificare automată a sistemului.

IV. DIPE asigură înrolarea în LAN a noului dispozitiv.

V. Instalarea și configurarea programelor de lucru se face la cererea angajatului AEP, cu aprobarea șefului direct al acestuia, prin completarea formularului din Anexa 1.
La instalarea fiecărui program care se accesează prin autentificare, DIPE se va asigura că acolo unde acesta permite acest lucru, opțiunea de schimbare automată a parolei la 6 luni va fi activată. Dacă acest lucru nu este posibil, DIPE va genera e-mail-uri de reamintire pentru schimbarea parolei.

VI. Toate privilegiile de acces la sistemele informatice sunt revocate imediat în momentul în care un angajat își încetează activitatea în cadrul AEP.

VII. DIPE ține evidența programelor instalate pe calculatoarele angajaților AEP. Evidența este constituită atât pe baza formularelor primite de DIPE, cât și pe baza auditului anual efectuat de DIPE.

6. Responsabilităţi

Nr. crt.	Compartimentul (postul) / acțiunea (operațiunea)	I	II	III	IV	V	VI	VII
1.	Angajat AEP			Ap		E		
2.	Compartiment AEP	E				A		
3.	DIPE		Ap		Ap	Ap	Ap	Ap

7. Formularul de evidență al modificărilor:

Nr. crt.	Ediție	Data ediției	Revizie	Data reviziei	Nr.pagină modificată	Descriere modificare	Semnătură conducător compartiment
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
PROCEDURĂ AFLATĂ LA PRIMA EDIȚIE							

8. Formularul de analiză a procedurii:

Nr. crt.	Compartiment	Nume și prenume conducător compartiment	Înlocuitor de drept sau delegat	Aviz favorabil		Aviz nefavorabil		
				Semnătură	Data	Observații	Semnătură	Data
1.	SG	[redacted]						
2.	SGA							
3.	SGA							
4.	DLCERPUE							
5.	DIPE							
6.	DCFPPCE							
7.	DLE							
8.	DCMAT							
9.	DSOE							
10.	DCI							
11.	DFC							
12.	DJ							
13.	DCA							

14.	DRU	[redacted]
15.	DT	
16.	DAP	
17.	DGR	
18.	DLCC	
19.	DAPI	
20.	SPIC	
21.	CCP	
22.	DIPE	
23.	DIPE	
24.	DIPE	
25.	DIPE	
26.	DIPE	
27.	DIPE	
28.	DIPE	
29.	DIPE	

9. Formularul de distribuire/difuzare:

	Scopul difuzării	Nr. exemplar	Compartiment	Nume și prenume	Data primirii	Semnătură	Data retragerii procedurii înlocuite	Semnătură	Data intrării în vigoare
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1.	Aplicare și difuzare personalului		DLCERPUE	[redacted]					
2.			DIPE						
3.			DCFPPCE						
4.			DLE						
5.	Aplicare și difuzare personalului		DCMAT						
6.			DSOE						
7.			DCI						
8.			DFC						
9.			DJ						
10.			DCA						
11.			DRU						

12.	Aplicare și difuzare personalului		DT	[redacted]
13.			DAP	
14.			DGR	
15.			DLCC	
16.			DAPI	
17.			SPIC	
18.			CCP	

10. Anexe

Anexa 1

AUTORITATEA ELECTORALĂ PERMANENTĂ
Compartiment: .....

APROBAT,
Director general DIPE

Formular pentru instalarea/actualizarea/dezinstalarea unui produs SOFTWARE

Subsemnatul/Subsemnata....., având funcția de ....., în cadrul ....., vă rog să-mi aprobați instalarea / actualizarea / dezinstalarea următoarelor produse SOFTWARE:

.....

.....

.....

Menționez că motivul solicitării este următorul:

.....

.....

.....

Data: ..... Semnătură solicitant: .....

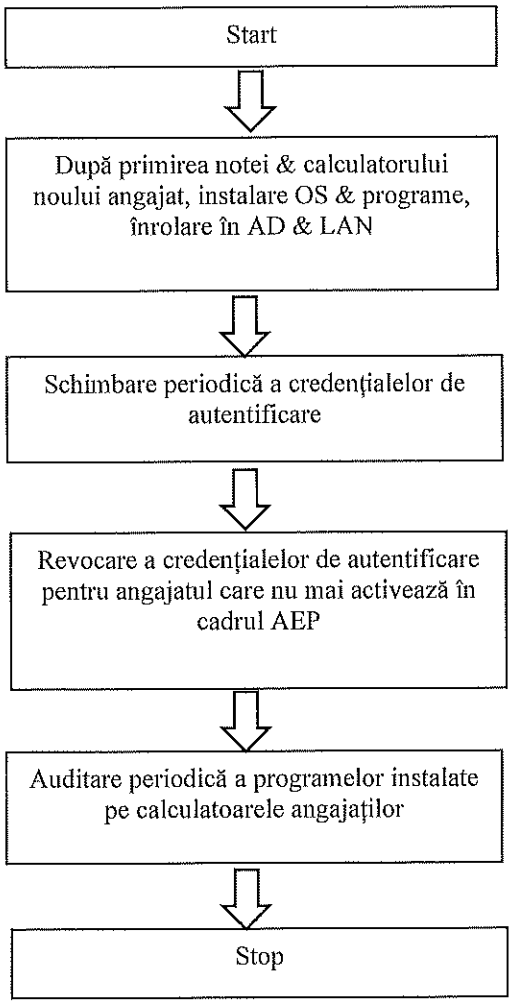
Propun aprobarea,

Şef Departament/Director general/Director/Şef serviciu/Şef birou

Nume şi prenume: .....

Semnătura: .....

Anexa 2 – Diagrama administrare utilizatori SIAEP



Anexa 3: Diagrama activităților de securitate