AVIZAT

PREȘEDINTE, COMISIA DE MONITORIZARE

Prof.univ.dr. Emil BĂLAN

PROPUN AVIZAREA

DIRECTOR, DIRECȚIA INFORMATICĂ

Conf.univ.dr. Andrei Găitănaru

SECURITATEA INFORMAȚIILOR ȘI A SISTEMULUI IT

Ediţia I

Cod: **PO-28**

Document aprobat prin Hotărârea de Senat din 18.02.2021

1. Lista responsabililor cu elaborarea, verificarea şi aprobarea ediţiei:

Nr. crt.	Acţiunea	Organism/ compartiment	Numele și prenumele	Funcția	Hotărâri, Avize, Decizii	Lună/an
1.	Elaborat	Direcția Informatică	Conf. Univ. Dr. Andrei Găitănaru	Director	Draft procedura PO-28	Octombrie 2020
2.	Verificat conform OSGG nr. 600/2018	Direcția Control Intern	Mariana Mureșan	Director		Ianuarie 2021
3.	Aviz de legalitate	Direcția Juridică	Lăcrămioara Pop Adriana Diana Stan	Director General Adm. Adj. Consilier juridic	Aviz juridic	Nr. 78 din 11 februarie 2021
4.	Verificat	Comisia de Monitorizare	Prof. univ. dr. Emil Bălan	Președinte	Aviz Președinte	11 februarie 2021
5.	Avizat Aprobat	Consiliul de Administrație Senat SNSPA			Decizie CA Hotărâre Senat	Nr. ……. Nr. …….

2. Situaţia ediţiilor şi a reviziilor în cadrul ediţiilor procedurii documentate

Nr. crt.	Ediţia/ Revizia	Componentă Revizuită	Temeiul reviziei	Data intrării în vigoare
1.	Ediţia I	Elaborarea Ediţiei iniţiale	Conform Ordin SGG nr. 600/2018	DeciziaCA nr……..
2.	Revizia 1	Elaborare Revizia 1		
3.	Revizia 2	Elaborare Revizia 2		

3. Lista cuprinzând persoanele la care se difuzează ediţia sau, după caz, revizia din cadrul ediţiei procedurii documentate

Nr. crt.	Scopul difuzării	Compartiment/ Organism	Funcţia
1.	Informare și aplicare	Direcția Informatică comunică/consiliază structurile/compartimentele SNSPA	Director IT
2.	Informare	Consiliul de Administrație, Senatul SNSPA	
3.	Arhivare	Direcția Control Intern	Secretar CM
4.	Coordonare, control	Comisia de Monitorizare	Preşedinte

4. Scopul procedurii

Procedura stabileşte politicile, principiile şi modalităţile de acţiune pentru asigurarea securităţii informaţiilor şi a sistemului IT din Școala Națională de Studii Politice și Administrative.

5. Domeniul de aplicare a procedurii documentate

Procedura se aplică de către Direcția Informatică și de persoanele altor compartimente/structuri din cadrul SNSPA, care sunt implicate, prin atribuțiile stabilite în fișa de post, în activitatea ce privește asigurarea securităţii informaţiilor şi a sistemului IT.

6. Documente de referinţă (reglementări) aplicabile activității procedurate

a) Ordinul SGG nr.600/2018 pentru aprobarea Codului controlului intern/managerial al entităților publice, cu modificarile si completarile ulterioare;

b) Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor);

c) Regulamentul (UE) 2016/679 al Parlamentului European si al Consiliului din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);

d) Strategia Națională privind Agenda Digitală pentru România 2020

e) RFC 1244 – Site Security Handbook:http://www.ietf.org/rfc/rfc1244.txt;

f) ISO 17799 – Standard detaliat de securitate:http://www.iso17799software.com/what.htm;

g) Decretul 165/2004 privind promulgarea Legii pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică;

h) Declaraţia privind libertatea comunicării pe Internet adoptată la Strasbourg în 2003;

i) Legea nr. 8/1996 -privind dreptul de autor şi drepturile conexe, cu modificările şi completările ulterioare;

j) Legea nr.455/2001-privind semnătura electronică, cu modificările şi completările ulterioare;

k) HG 1007/2001-privind aprobarea strategiei guvernului privind informatizarea administrației publice;

l) Legea 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare;

m) Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, cu modificările şi completările ulterioare;

n) Regulamentul (UE) al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE;

o) Directiva (UE) 2016/680 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului;

p) Ghidul privind Responsabilul cu protecția datelor (DPO) – www.dataprotection.ro;

q) Legea nr.363/2018 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date;

r) Legea educaţiei naţionale nr.1/2011, cu modificările şi completările ulterioare;

7. Definiţii şi abrevieri ale termenilor utilizaţi

7.1 Definiţii:

Nr. Crt.	**Termenul**	**Definiţia şi/sau, dacă este cazul, actul care defineşte termenul**
1	Activitate procedurală	Proces major sau activitate semnificativă pentru care se pot stabili reguli şi modalităţi de lucru, general valabile, în vederea îndeplinirii, în condiţii de regularitate, eficiență, eficacitate și economicitate a obiectivelor structurii/compartimentului și/sau universității.
2	Actualizare procedura	Constă fie în revizuirea procedurii fie în elaborarea unei noi ediți.
4	Compartiment (Structură)	Facultate / direcție / serviciu / birou/ compartiment cu coordonator;
5	Conducător structură/compartiment	Decan/ director / şef serviciu/ şef birou/ șef alte structuri;
6	Control intern managerial	Ansamblul formelor de control exercitate la nivelul entităţii publice, inclusiv auditul intern, stabilite de conducere în concordanţă cu obiectivele acesteia şi cu reglementările legale, în vederea asigurării administrării fondurilor în mod economic, eficient şi eficace; acesta include, de asemenea, structurile organizatorice, metodele şi procedurile. Sintagma "control intern managerial" subliniază responsabilitatea tuturor nivelurilor ierarhice pentru ţinerea sub control a tuturor proceselor interne desfăşurate pentru realizarea obiectivelor generale şi a celor specifice.
7	Delegare	Procesul de atribuire de către un conducător de entitate și/sau compartiment, pe o perioadă limitată, a unora dintre sarcinile sale unui subordonat, împreună cu competenţele şi responsabilităţile aferente.
8	Diagrama de proces	Schema logică cu forme grafice care reprezintă etapele și pașii realizării unui proces sau unei activități.

9	Ediţie procedură	Forma actuală a procedurii; ediția unei proceduri se modifică atunci când deja au fost realizate de regulă treirevizii ale respectivei proceduri sau atunci când modificările din structura procedurii depășesc 50% din conținutul reviziei anterioare.
10	Fișa postului	Document care defineşte locul şi contribuţia postului în atingerea obiectivelor individuale şi organizaţionale, caracteristic atât individului, cât şi entităţii şi care precizează sarcinile şi responsabilităţile care îi revin titularului unui post.
11	Măsuri de control	Acţiuni stabilite pentru gestionarea riscurilor și monitorizarea permanentă sau periodică a unei activităţi(situaţii).
12	Monitorizare	Acțiune continuă de colectare a informaţiilor relevante, despre modul de desfăşurare a unui proces sau a unei activităţi.
13	Obiectiv	Descrie un rezultat aşteptat sau un impact şi rezumă motivele pentru care au fost întreprinse o serie de acţiuni.
16	Obiective specifice	Derivate din obiective generale şi care descriu, de regulă, rezultate sau efecte așteptate ale unor activităţi care trebuie atinse pentru ca obiectivul general corespunzător să fie îndeplinit.
17	Procedură documentată	Modul specific de realizare a unei activități sau a unui proces, editat pe suport de hârtie sau în format electronic; procedurile documentate pot fi proceduri de sistem şi proceduri operaţionale.
18	Procedură de sistem (procedură general)	Descrie un proces sau o activitate care se desfăşoară la nivelul entității publice aplicabil/aplicabilă majorității sau tuturor compartimentelor, dintr-o entitate publică.
19	Procedură operaţională (procedură de lucru)	Procedură care descrie un process sau o activitate care se desfăşoară la nivelul uneia sau mai multor structuri/compartimente, fără aplicabilitate la nivelul întregii universități.

20	Proces	Un flux de activităţi sau o succesiune de activităţi logic structurate șiorganizate, în scopul atingerii unor obiective definite.
21	Responsabilitate	Obligaţia de a îndeplini sarcina atribuită, a cărei neîndeplinire atrage osancţiune corespunzătoare, după caz.
22	Responsabilitate managerială	Defineşte un raport juridic de obligaţie a îndeplinirii sarcinilor de către conducătorulentităţii publice sau al unei structuri organizatorice a acesteia, care presupune să exercite managementul în limitele unor determinări interne şi externe, în scopul realizării eficace, eficiente şi în conformitate cu dispoziţiile legale a obiectivelor stabilite.
24	Resurse	Totalitatea elementelor de natură fizică, tehnică, umană, informaţională şi financiară, necesare ca input pentru ca strategiile să fie operaţionale.
26	Virus informatic	Un program care se ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte deranjante sau distructive. Un virus se execută în momentul în care este accesat un fişier infectat.
27	Vierme	Un program care se auto-copiază în spaţiul de stocare al unui sistem informatic şi care se răspândeşte către alte calculatoare prin intermediul reţelei. Unii dintre aceşti viermi reprezintă o ameninţare la adresa securităţii informatice datorită faptului că folosesc reţeaua pentru a se multiplica, determinând nefuncţionarea sau funcţionarea defectuoasă a reţelei.
28	Cal troian	Virus sau vierme care este disimulat sub forma unui program atractiv sau inofensiv. Acesta se poate răspândi prin email, prin utilizarea unui stick de memorie sau prin descarcarea din retea a unor fisiere compromise.

29	Phishing	Are loc când se încearcă inducerea în eroare a unui utilizator, astfel încât acesta să furnizeze online informaţii de identificare sau cu caracter personal. De obicei, *phishing*-ul are loc prin email sau prin site-uri care arată similar cu site-uri cunoscute.
30	Ransoms	*Malware* care blochează computerul sau criptează fişierele. De obicei pentru deblocarea sistemului şi/sau recuperarea fişierelor se solicit plăţi în scopul declarat de furnizare ulterioară a cheilor de decriptare, neexistând nicio garanţie că datele vor fi recuperate în acest mod.
31	Incident de securitate	Eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrităţii şi/sau confidenţialităţii informaţiei de pe un sistem informatic automatizat. Aceasta include examinarea sau navigarea neautorizată, întreruperea sau anularea unui serviciu, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea informaţiilor, modificarea informaţiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software.
32	Expunere	Reducerea constrângerilor impuse pentru accesarea informaţiilor.
33	Vulnerabilitate	Slăbiciune care poate fi exploatată în scopul accesării neautorizate a resurselor sau a informaţiilor.
34	Atac	Încercarea de a exploata vulnerabilitatea.
35	Control	Măsură de gestionare a vulnerabilităţii de obicei în scopul reducerii expunerii la riscuri.

7.2 Abrevieri

Nr. Crt.	Abrevierea	Termenul abreviat
1.	PS	Procedură de sistem
2.	PO	Procedura operaţională
3.	SNSPA	Școala Națională de Științe Politice și Administrative
4.	SGG	Secretariatul General al Guvernului
5.	CM	Comisia de monitorizare
6.	DCI	Direcția Control Intern
7.	SPS	Direcția Secretariat, Senat, CA, Proiecte Strategice

8. Descrierea procedurii documentate

8.1 Generalități

Politica de securitate a resurselor informatice are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei.

a) *Confidenţialitatea* se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primate sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul SNSPA, sunt proprietatea instituţiei în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la resursele informatice.

b) *Integritatea* se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau a distrugerii neautorizate.

c) *Disponibilitatea* se asigură prin funcţionarea continuă a tuturor componentelor sistemului şi resurselor informatice. Aplicaţiile informatice au nevoie de niveluri diferite de disponibilitate în funcţie de impactul sau de daunele ce pot fi produse ca urmare a nefuncţionării lor corespunzătoare. Politica de securitate are ca scop stabilirea cadrului necesar pentru elaborarea regulamentelor şi a procedurilor de securitate. Acestea sunt obligatorii pentru toţi utilizatorii resurselor informatice.

8.2 Politica de Securitate în utilizarea resurselor informatice din cadrul SNSPA

8.2.1 Scopul elaborării politicii de Securitate informaţională

a) Politica de Securitate are ca scop stabilirea cadrului necesar pentru elaborarea regulamentelor şi a procedurilor de securitate;

b) Politica de securitate este implementată prin reguli şi măsuri menite să asigure securitatea informaţiilor specific instituţiei;

c) reglementările rezultate din politica de Securitate sunt obligatorii pentru toţi utilizatorii resurselor informatice.

8.2.2 Planul de asigurare a securităţii informaţionale a reţelei IT

La întocmirea planului de asigurare a securităţii informaţionale a reţelei IT se au în vedere tipurile posibile de ameninţări şi/sau acţiuni:

a) **Forţa majoră**: pierderea personalului, inundaţie, incendiu;

b) **Deficienţe de organizare**: utilizarea incorectă sau neadecvată a resurselor IT, folosirea neautorizată a drepturilor de utilizare;

c) **Greşeli umane**: distrugerea din neglijenţă a unor echipamente sau a unor date, nerespectarea măsurilor de Securitate, defecţiuni datorate acţiunilor improprii ale personalului de întreţinere sau de intervenţie, administrarea necorespunzătoare a sistemului de Securitate implementat, organizarea defectuoasă a gestionării informaţiilor şi a datelor;

d) **Defecţiuni tehnice**: indisponibilitatea surselor de alimentare cu energie electrică, parametri improprii ai energiei electrice, nefuncţionarea sistemelor de stocare/înregistrare a datelor, existenţa unor vulnerabilităţi ale programelor folosite, acces impropriu la mecanismul ethnic de gestiune a securităţii informaţionale;

e) **Acte deliberate**: manipularea sau distrugerea echipamentului de protecţie a reţelei sau a accesoriilor sale, manipularea frauduloasă a datelor sau a programelor informatice, furt, interceptarea canalelor şi a

liniilor de date ale infrastructurii, accesarea și/sau modificarea neautorizată a sistemului de protecţie a reţelei, încercarea sistematică de descoperire a parolelor de acces, utilizarea abuzivă a drepturilor de utilizator, limitarea sau blocarea drepturilor de administrare, facilitarea pătrunderii de viruşi/troieni informatici în reţea, furtul de identitate şi accesarea unor drepturi pentru care nu există autorizare, urmărirea traficului de date, blocarea prin diverse metode a unor servicii sau porturi de date.

8.3 Reguli de utilizare corectă a resurselor informatice

a) Utilizatorii trebuie să anunţe Departamentul IT în cazul în care se observă orice problemă sau breşă în sistemul de Securitate al SNSPA, cât şi orice posibilă întrebuinţare greşită sau încălcarea regulamentului.
b) Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip din sistem.
c) Utilizatorii nu trebuie să încerce să obţină acces la date sau programe pentru care nu au autorizaţie sau consimţământ explicit.
d) Utilizatorii nu trebuie să divulge sau să înstrăineze datele de autentificare proprii (nume de conturi, parole etc.), utilizate în scopuri de autorizare şi identificare în reţeaua informaţională a instituţiei.
e) Utilizatorilor nu le este permis să realizeze copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).
f) Se recomandă ca utilizarea de programe de tip *shareware* sau *freeware* să se facă cu responsabilitate, eventual cu consultarea Departamentului IT dacă se consideră necesar.
g) Utilizatorii nu trebuie să descarce, să instaleze şi să ruleze programe de penetrare a unor restricţii de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii sistemului informatic al instituţiei.
h) Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care instituţia le poate considera ofensive, indecente sau obscene.
i) Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor SNSPA folosind resursele informatice.

8.4 Accesul fizic

Toate încăperile în care sunt instalate echipamente ale sistemului informatic trebuie să fie protejate la accesarea fizică neautorizată, în funcţie de importanţa acestora şi de tipul datelor vehiculate sau stocate.

8.5 Confidențialitatea serviciilor informatice

a) În scopul administrării sistemului informatic şi pentru asigurarea securităţii acestuia personalul autorizat poate monitoriza activitatea din reţeaua de date cu respectarea confidenţialităţii, în conformitate cu legile în vigoare.
b) Utilizatorii trebuie să informeze Departamentul IT în legătură cu eventualele suspiciuni de încălcare a confidenţialităţii şi să ofere, dacă este posibil, informaţiile necesare pentru identificarea problemei.
c) Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicare ale terţilor nu poate fi asigurată implicit. Pentru astfel de situaţii, asigurarea confidenţialităţii şi integrităţii informaţiilor sensibile este o obligaţie a utilizatorilor şi are la bază folosirea tehnicilor de securizare (criptare, conexiuni VPN).

8.6 Configurarea parametrilor de acces la rețea

a) Reţeaua informatică a SNSPA este administrată de către Departamentul IT care este responsabil cu întreţinerea şi dezvoltarea acesteia.
b) Toate echipamentele conectate la reţea vor fi configurate conform specificaţiilor IT.
c) Reţeaua locală IT este de tip Ethernet și suportă un set de protocoale de comunicaţie de reţea în conformitate cu scopul şi misiunea instituţiei.
d) Adresele de reţea sunt gestionate centralizat exclusiv de către Departamentul IT;
e) Utilizatorii nu au dreptul să extindă sau să retransmită în niciun fel serviciile reţelei SNSPA.
Este interzisă instalarea de echipamente (*router, switch, hub* sau punct de acces) în reţeaua Intranet SNSPA fără avizul IT.

8.7 Monitorizarea resurselor informatice

a) Monitorizarea reţelei se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice şi a situaţiilor de încălcare a regulamentelor de securitate.

b) Fişierele jurnal vor fi stocate şi vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi a abaterilor de la regulamentele de securitate ale instituţiei.

8.8 Securitatea serverelor

a) Un server nu trebuie conectat la reţeaua instituţiei decât atunci când este securizat adecvat.

b) Procedura de securizare a serverelor include obligatoriu următoarele:

1.instalarea sistemului de operare dintr-o sursă veridică, aprobată;

2.aplicarea *patc*h-urilor furnizate de producător;

3.înlăturarea programelor, a serviciilor sistem şi a driverelor care nu sunt necesare;

4.setarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare

5.dezactivarea sau schimbarea parolelor predefinite;

6.securizarea accesului la servicii din Internet;

7.securizarea accesului fizic la echipamente.

8.9 Parole de acces

a) Toate parolele trebuie să îndeplinească următoarele condiţii:

1.Să fie schimbate de utilizator în mod regulat;

2.Să aibă o lungime, în număr de caractere, cat mai mare;

3.Să aibă diversitate cât mai mare ca şi caractere utilizate;

4.Reutilizarea parolelor este interzisă;

5.Parolele stocate trebuie securizate;

6.Parolele de cont utilizator nu trebuie divulgate către terţi sub nici o formă, fără excepţie;

b) Dacă se suspectează că o parole a fost divulgată, aceasta trebuie schimbată imediat;

c) Este recomandabil ca utilizatorii să nu folosească programe de stocare a parolelor;

d) Calculatoarele nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea pe bază de parolă;

8.10 Proceduri de schimbare a parolei asistate de administratorul de sistem

1. Utilizatorul se va legitima, iar administratorul de sistem va verifica drepturile de acces ale persoanei la contul utilizator;
2. Se va genera o parolă care va fi comunicată utilizatorului;
3. Utilizatorul va schimba parola temporară, comunicată anterior, în cel mai scurt timp posibil.

8.11 Recomandări pentru alegerea parolelor

a) Parolele trebuie să fie schimbate după cel mult șase luni de utilizare;

b) Parolele trebuie să aibă o lungime minimă recomandată de nouă caractere;

c) Parolele trebuie să conţină o varietate cât mai mare de caractere (litere mici şi mari, caractere numerice şi caractere speciale acolo unde sistemul permite).

d) Parolele trebuie să respecte următoarele condiţii:

-nu trebuie să coincidă sau să fie asemănătoare cu numele de utilizator (*login*-ul);

-nu trebuie să coincidă sau să fie asemănătoare cu numele utilizatorului;

-nu trebuie să coincidă cu date personale (codul numeric personal, data naşterii, numele străzii/oraşului, numărul de telefon etc.);

-parolele trebuie tratate ca informaţie confidenţială şi nu trebuie divulgate în nicio situaţie.

8.12 Sistemul de mesagerie electronică

a) Următoarele activităţi sunt interzise:

-trimiterea de mesaje cu caracter de intimidare sau hărţuire;

-folosirea sistemului de mesagerie electronică în alte scopuri decât cele profesionale;

-încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;

-folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile în care persoana este autorizată administrative în acest scop;

-folosirea programelor de poştă electronică neautorizate.

8.13 Instruire și informare

a) Informarea angajaţilor poate fi făcută la angajare, periodic sau de câte ori este nevoie.

Este importantă comunicarea modificărilor realizate în politicile de securitate, datorate eventualelor modificări legislative;

b) Instruirea angajaţilor cu privire la riscurile care conduc la o utilizare necorespunzătoare, intenţionată sau neintenţionată. Angajaţii trebuie să cunoască, care sunt ameninţările, cum pot fi eliminate riscurile, eventualele probleme legale generate de utilizările necorespunzătoare.

8.14 Monitorizare

a) Activităţile utilizatorilor în cadrul reţelei de date şi care implică accesul şi/sau folosirea sistemului informatic al SNSPA pot fi înregistrate şi analizate.

b) Înregistrările activităţilor de utilizare a sistemului informatic al SNSPA sunt folosite exclusiv în scopul identificării acţiunilor ilegale sau abusive şi respectă criteriile de confidenţialitate instituţională şi personală.

8.15 Măsuri și reguli pentru asigurarea securității sistemului informatic

Măsuri generale de securitate:

a) Asigurarea alimentării sigure cu energie electrică folosind surse de alimentare neîntreruptibile;

b) Realizarea de verificări şi revizii tehnice periodice;

c) Interzicerea utilizării de programe neautorizate;

d) Utilizarea de parole conforme şi schimbarea periodică a acestora;

e) Identificarea permanentă a vulnerabilităţilor sistemelor de protecţie;

f) Verificarea periodică a nivelului de securitate a reţelei (audit de securitate informaţională);

g) Educarea personalului în legătură cu măsurile de securitate necesare şi instruirea acestuia pentru utilizarea de programe specifice;

h) Verificarea periodică a sistemelor cu ajutorul programelor anti-virus şi asigurarea actualizării permanente a listelor cu definiţiile viruşilor;

i) Autentificarea în reţea trebuie asigurată numai prin conexiuni de date securizate;

j) Gestiunea corectă a copiilor de rezervă (*back-up*) în ceea ce priveşte securitatea, integritatea şi disponibilitatea acestora prin verificarea permanentă a funcţionalităţii mediilor de păstrare a datelor şi a nealterării conţinutului;

8.16 Reguli de bază pentru utilizatorii individuali ai sistemelor din rețea:

a) Utilizatorii reţelei trebuie să salveze periodic datele importante cu care lucrează (documente, imagini, baze de date etc.) pe un suport extern. Suportul extern se va deconecta de la calculator după ce se finalizează operaţiunea de copiere, iar acesta va fi păstrat într-un loc sigur;

b) Utilizatorii pot solicita instruirea pentru folosirea în siguranţă a staţiei de lucru şi pentru deprinderea modalităţilor de salvare periodică a datelor de interes;

c) Utilizatorii sistemelor vor urmări actualizarea periodică a sistemului de operare, a programului antivirus instalat, precum şi actualizarea altorap licaţii software utilizate, dacă este cazul;

d) Utilizatorii nu vor instala pe staţiile pe care lucrează programe neautorizate, programe fără licenţă

sau pentru care nu există drepturi legale de utilizare sau aplicaţii care nu au legătură cu activitatea profesională desfăşurată în cadrul instituţiei;

e) Utilizatorii vor folosi pentru transmiterea/primirea de mesaje electronice de serviciu adresele email instituţionale definite în domeniile/subdomeniile administrate de universitates (ex: utilizator@snspa.ro, utilizator@[structura academica].ro);

f) Se va evita utilizarea memoriilor externe de tip flash (stick de date) pentru a reduce expunerea la viruşi informatici atât a staţiei proprii de lucru cât şi a reţelei SNSPA;

g) Atunci când este posibil utilizatorul va verifica credibilitatea sursei unui mesaj email şi va investiga formal autenticitatea acestuia, evitând deschiderea fişierelor ataşate suspecte;

8.17 Utilizarea dispozitivelor conectate la reţea (routere wireless, sisteme DVR, camere IP, echipamente de măsură, sisteme SmartTV etc)

a) Parolele implicite (*default*) de pe dispozitive vor fi înlocuite imediat ce este posibil;

b) *Firmware*-ul dispozitivelor trebuie să fie permanent actualizat;

c) Opţiunile de tip *remote management* trebuie să fie limitate la strictul necesar pentru administrare.

8.18 Reguli de securitate şi conectare la reţeaua wireless

a) Accesul wireless în reţeaua SNSPA se realizează în mod obişnuit prin autentificare;

b) În condiţii bine definite este posibil accesul public de tip guest;

c) Este recomandată evitarea utilizării conexiunilor necriptate;

d) Router-ele instalate în spațiile SNSPA trebuie să fie configurate şi securizate conform recomandărilor Departamentului IT, fiind interzisă conectarea router-elor sau a punctelor de acces fără avizul Departamentului IT;

e) Router-ele şi punctele de acces, altele decât cele administrate de Departamentul IT şi destinate accesului public cu/fără autentificare vor fi definite (SSID) într-o manieră care să permită identificarea acestora şi a amplasamentului lor fizic (corp clădire, număr sală/birou);

8.19 Politica de Securitate a dispozitivelor mobile (telefoane, tablete)

a) Sistemul de operare şi aplicaţiile utilizate trebuie să fie actualizate periodic;

b) Se recomandă conectarea doar la *router-e wireless* securizate (cu parolă);

c) Dispozitivele mobile nu vor avea alocate adrese IP fixe, alocarea acestora se face automat în reţeaua wireless.

8.20 Monitorizarea eficienţei reţelei informatice

Protecţia eficientă a reţelei informatice a instituţiei conduce la creşterea indicatorilor de performanţă asociaţi utilizării acesteia şi la îmbunătăţirea gradului de satisfacţie a beneficiarilor direcţi.

Indicatori urmăriţi:

a) eficienţa accesului la resurse electronice de informare, comunicare electronică şi transfer de date;
b) nivelul de performanţă al echipamentelor de comunicaţie şi al infrastructurii de date;
c) gradul de creştere a operativităţii îndeplinirii sarcinilor de către salariaţi;
d) gradul de diminuare a timpului necesar elaborării documentelor standard;
e) gradul de creştere a operativităţii în furnizarea de informaţii sau documente către solicitanţi;
f) nivelul general de satisfacţie al utilizatorilor reţelei de date SNSPA.

8.21 Resurse necesare:

Resurse materiale

a) mobilier pentru personalul comisiei şi pentru solicitanţi;
b) mobilier pentru stocarea dosarelor;
c) aparatură și echipamente specifice;
d) rețea internet;
e) rețea intranet;
f) telefoane, faxuri;
g) alte dotări necesare.

Resurse umane

a) Comisia de monitorizare

b) Angajații Departamentului IT;

c) Personalul compartimentelor implicate în desfăşurarea activităţii;

d) Alte părţi interesate.

Resurse financiare

a) Conform Bugetului de venituri și cheltuieli al Şcolii Naţionale de Studii Politice şi Administrative pentru anul în curs.

9. Responsabilităţi şi răspunderi în derularea activităţii

9.1 Departamentul IT:

a) creează condiţiile de aplicare a prezentei proceduri;

b) monitorizează permanent nivelul de securitate informaţională şi propune măsuri de optimizare;

c) numeşte responsabili care să asigure elaborarea, modificarea şi gestionarea procedurilor specific în cadrul serviciului;

d) răspunde de configurarea rețelei informatice în conformitate cu politica de Securitate IT;

e) stabilește resursele (hardware, software, licențe, servicii) necesare funcționării în bune condiții a rețelei informatice;

f) asigură managementul conturilor;

g) securitatea datelor cu caracter personal - GDPR;

i) asigură upgrade hardware;

j) asigură instruirea utilizatorilor în ceea ce privește accesul la/și utilizarea resurselor informatice;

k) intervenția operativă pentru rezolvarea problemelor apărute în rețeaua informatică a SNSPA.

9.2 Utilizatori:

a) Utilizatorii trebuie să anunțe Departamentul IT dacă apare orice problemă sau breșă apărută în sistemul informatic și orice posibilă întrebuințare greșită a regulamentelor în vigoare;
b) Utilizatorii nu trebuie să compromită protecția sistemelor informatice și de comunicații și nu trebuie să afecteze prin acțiunile lor confidențialitatea, integritatea și disponibilitatea informațiilor în cadrul SNSPA;
c) Utilizatorii nu trebuie să încerce să obțină acces la date sau programe pentru care nu sunt autorizați;
d) Utilizatorii nu trebuie să divulge nume de conturi, parole, numere de identificare personal (PIN-uri), informații similar în scopuri de autorizare și funcționare;
e) Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor SNSPA folosind sistemul informatic.

9.3 Direcția Juridică:

a) aduce la cunoştinţa conducerii compartimentelor apariţia sau modificarea actelor care reglementează sau legiferează activităţile specifice;

10. Cuprins

Nr. crt.	Denumirea componentei din cadrul procedurii	Nr. pag.
Pagină de gardă		1
1	Lista responsabililor cu elaborarea, verificarea şi aprobarea ediţiei	2
2	Situaţia ediţiilor şi a reviziilor în cadrul ediţiilor procedurii	3
3	Lista cuprinzând persoanele la care se difuzează ediţia sau, după caz, revizia din cadrul ediţiei procedurii	3
4	Scopul procedurii documentate	4
5	Domeniul de aplicare a procedurii documentate	4
6	Documente de referinţă aplicabile activităţii procedurate	4
7	Definiţii şi abrevieri ale termenilor utilizaţi	6
8	Descrierea procedurii documentate	6
	8.1 Generalități	10
	8.2 Politica de securitate în utilizarea resurselor informatice în cadrul SNSPA	11
	8.2.1 Scopul elaborării politicii de Securitate informaţională	11
	8.2.2 Planul de asigurare a securităţii informaţionale a reţelei IT	11
	8.3 Reguli de utilizare corectă a resurselor informatice	12
	8.4 Accesul fizic	13
	8.5 Confidențialitatea serviciilor informatice	13
	8.6 Configurarea parametrilor de acces la rețea	13
	8.7 Monitorizarea resurselor informatice	14
	8.8 Securitatea serverelor	14
	8.9 Parole de acces	14
	8.10 Proceduri de schimbare a parolei asistate de administratorul de sistem	15
	8.11 Recomandări pentru alegerea parolelor	15
	8.12 Sistemul de mesagerie electronică	16
	8.13 Instruire și informare	16
	8.14 Monitorizare	16
	8.15 Măsuri și reguli pentru asigurarea securității sistemului informatic	17
	8.16 Reguli de bază pentru utilizatorii individuali ai sistemelor din rețea	17
	8.17 Utilizarea dispozitivelor conectate la reţea	18
	8.19 Politica de Securitate a dispozitivelor mobile	19
	8.20 Resurse necesare	19
9	Responsabilităţi şi răspunderi în derularea activităţii	20
	9.1 Departamentul IT	20
	9.2 Utilizatori	21
	9.3 Direcția Juridică	21
10	Cuprins	22