



Universitatea
Ștefan cel Mare
Suceava

Cod: **PO-SCTI-03**

Ediția: 1

Revizia: 0

PROCEDURĂ OPERAȚIONALĂ privind securitatea informațiilor și a sistemului IT

Această procedură a fost aprobată în

Ședința Consiliului de Administrație din data de 17.01.2017

Rector,

Prof.univ.dr.ing. Valentin POPA

	Numele și prenumele	Funcția	Data	Semnătura
Elaborat	Vultur Oana Mihaela	Inginer de sistem	17.12.2016	
Verificat	Potorac Alin Dan	Coordonator SCTI	21.12.2016	
Avizat	Velicu Cătălin	Director General Administrativ	17.01.2017	

Cuprins

1. SCOPUL PROCEDURII	3
2. DOMENIUL DE APLICARE	3
3. DOCUMENTE DE REFERINȚĂ	3
4. DEFINIȚII ȘI ABREVIERI	3
4.1 Termeni și definiții	3
4.2 Abrevieri	4
5. CONȚINUT	4
5.1 Principiile asigurării securității informaționale	4
5.2 Politica de securitate în utilizarea resurselor informatice din cadrul USV	5
5.3 Măsuri și reguli pentru asigurarea securității sistemului informatic	8
5.4 Monitorizarea eficienței rețelei informatice	10
6. RESPONSABILITĂȚI	10
7. DISPOZIȚII FINALE	10
8. ANEXE	11

1. SCOPUL PROCEDURII

Procedura stabilește politicile, principiile și modalitățile de acțiune pentru asigurării securității informațiilor și a sistemului IT din Universitatea „Ștefan cel Mare” din Suceava.

2. DOMENIUL DE APLICARE

Procedura se aplică în cadrul Serviciului de Comunicații și Tehnologii Informaționale din Universitatea Ștefan cel Mare din Suceava

3. DOCUMENTE DE REFERINȚĂ

3.1. Reglementări internaționale

- 3.3.1 RFC 1244 – Site Security Handbook: <http://www.ietf.org/rfc/rfc1244.txt>
- 3.3.2 ISO 17799 – Standard detaliat de securitate: <http://www.iso17799software.com/what.htm>
- 3.3.3 Convenția privind criminalitatea informatică - Monitorul Oficial, Partea I nr. 343 din 20/04/2004
- 3.3.4 Declarația privind libertatea comunicării pe Internet adoptată la Strasbourg în 2003

3.2. Legislație primară

- 3.2.1 Legea nr. 8/1996 - privind dreptul de autor și drepturile conexe, cu modificările și completările ulterioare
- 3.2.2 Lege nr. 455/2001 - privind semnătura electronică, cu modificările și completările ulterioare
- 3.2.3 Lege nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare
- 3.2.4 HG nr. 1007/2001 - privind aprobarea strategiei guvernului privind informatizarea administrației publice
- 3.2.5 Legea 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare;

3.3. Legislație secundară

- 3.3.1 Norma tehnică și metodologică din 13 decembrie 2001 pentru aplicarea Legii nr. 455/2001 privind semnătura electronică
- 3.3.2 Recomandare MCTI - Ghid privind realizarea paginilor web pentru autoritățile și instituțiile administrației publice centrale și locale

4. DEFINIȚII ȘI ABREVIERI

4.1 Termeni și definiții

- 4.1.1 **Virus informatic** - Un program care se atașează la un fișier executabil sau la o aplicație vulnerabilă și care generează efecte deranjante sau distructive. Un virus se execută în momentul în care este accesat un fișier infectat.
- 4.1.2 **Vierme** - Un program care se auto-copiază în spațiul de stocare al unui sistem informatic și care se răspândește către alte calculatoare prin intermediul rețelei. Unii dintre acești viermi reprezintă o amenințare la adresa securității informatice datorită faptului că folosesc rețeaua pentru a se multiplica, determinând nefuncționarea sau funcționarea defectuoasă a rețelei.

- Spre deosebire de un virus informatic, un vierme nu are nevoie să se atașeze la anumite fișiere pentru a se multiplica.
- 4.1.3 **Cal troian** – Este obicei un virus sau un vierme care este disimulat sub forma unui program atractiv sau inofensiv. Acesta se poate răspândi prin email, prin utilizarea un stick de memorie sau prin descarcarea din rețea a unor fișiere compromise.
- 4.1.4 **Phishing** – un atac de *phising* are loc atunci când se încearcă inducerea în eroare a unui utilizator astfel încât acesta să furnizeze online informații de identificare sau cu caracter personal. De obicei, *phishing*-ul are loc prin e-mail sau prin site-uri care arată similar cu site-uri cunoscute.
- 4.1.5 **Ransoms** – este un *malware* care blochează computerul sau criptează fișierele. De obicei pentru deblocarea sistemului și/sau recuperarea fișierelor se solicită plăți în scopul declarat de furnizare ulterioară a cheilor de decriptare, neexistând însă nicio garanție că datele vor fi recuperate în acest mod.
- 4.1.6 **Incident de securitate** - În termeni informatici este definit ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrității și/sau confidențialității informației 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 informațiilor, modificarea informațiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără știința sau intenția utilizatorului.
- 4.1.7 **Expunere** - Reducerea a constrângerilor impuse pentru accesarea informațiilor.
- 4.1.8 **Vulnerabilitate** - Slăbiciune care poate fi exploatată în scopul accesării neautorizate a resurselor sau informațiilor.
- 4.1.9 **Atac** - Încercarea de a exploata vulnerabilitatea.
- 4.1.10 **Control** - Măsură de gestionare vulnerabilității de obicei în scopul reducerii expunerii la riscuri.

4.2 Abrevieri

USV	– Universitatea Ștefan cel Mare din Suceava
SCTI	– Serviciul de Comunicații și Tehnologii Informaționale

5. CONȚINUT

5.1 Principiile asigurării securității informaționale

- 5.1.1 Principiile care trebuie îndeplinite pentru a asigura securitatea sistemelor informatice sunt:
- Principiul responsabilității.** Responsabilitățile legate de securitate informațională pentru deținători, furnizori și utilizatori de sisteme informatice sau servicii de date trebuie să fie explicite.
 - Principiul conștientizării.** Pentru a asigura securitatea sistemelor informatice, deținătorii, furnizorii și utilizatorii acestora trebuie să poată accesa și dobândi cunoștințele necesare, să fie informați despre existența și cadrul general al măsurilor, practicilor și procedurilor de securitate a sistemelor informatice și să poată acționa voluntar pentru reducerea riscurilor.
 - Principiul eticii.** Sistemele informatice și securitatea sistemelor informatice trebuie folosite într-o manieră în care drepturile și interesele legale ale celorlalți să nu fie afectate.
 - Principiul multidisciplinarității.** Măsurile, practicile și procedurile de asigurare a securității sistemelor informatice trebuie să țină cont de toate considerațiile și aspectele

relevante, inclusiv tehnice, administrative, organizaționale, operaționale, comerciale, educaționale și legale.

- e) **Principiul proporționalității.** Nivelurile de securitate, costurile, măsurile, practicile și procedurile trebuie să fie corespunzător dimensionate și proporționale cu valoarea și gradul de încredere necesar pentru fiecare tip de informație avându-se în vedere de asemenea și nivelul daunelor potențiale respectiv probabilitatea de apariție a acestora.
- f) **Principiul integrării.** Măsurile, practicile și procedeele de asigurare a securității sistemelor informatice trebuie să fie coordonate instituțional și integrate și cu alte măsuri, practici și procedee ale organizației cu scopul creării unui sistem global de securitate informațională coerent.
- g) **Principiul actualității.** Instituțiile, indiferent de tipul lor, trebuie să acționeze rapid și într-o manieră coordonată pentru a preveni și a răspunde eficient la apariția breșelor de securitate a sistemelor informatice.
- h) **Principiul reevaluării.** Securitatea sistemelor informatice trebuie analizată și reevaluată periodic pentru a răspunde celor mai noi tipuri de agresiuni informatice.
- i) **Principiul democrației.** Securitatea sistemelor informatice trebuie să nu restrângă drepturile de utilizare legitimă a rețelelor de date.

5.1.2 Politica de securitate a resurselor informatice are ca scop asigurarea integrității, confidențialității și disponibilității informației.

- a) *Confidențialitatea* se referă la protecția datelor împotriva accesului neautorizat. Fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia și sub controlul USV, sunt proprietatea instituției în condițiile legilor în vigoare. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la resursele informatice.
- b) *Integritatea* se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.
- c) *Disponibilitatea* se asigură prin funcționarea continuă a tuturor componentelor sistemului și resurselor informatice. Aplicațiile informatice au nevoie de niveluri diferite de disponibilitate în funcție de impactul sau daunele ce pot fi produse ca urmare a nefuncționării lor corespunzătoare. Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor și procedurilor de securitate. Acestea sunt obligatorii pentru toți utilizatorii resurselor informatice.

5.2 Politica de securitate în utilizarea resurselor informatice din cadrul USV

5.2.1 Scopul elaborării politicii de securitate informațională

- a) Politica de securitate are ca scop stabilirea cadrului necesar pentru elaborarea regulamentelor și procedurilor de securitate;
- b) Politica de securitate este implementată prin reguli și măsuri menite să asigure securitatea informațiilor specifice instituției;
- c) reglementările rezultate din politica de securitate sunt obligatorii pentru toți utilizatorii resurselor informatice.

5.2.2 La întocmirea planului asigurare a securității informaționale a rețelei IT se au în vedere tipurile posibile de amenințări și/sau acțiuni:

- a) **Forța majoră:** pierderea personalului; inundație; incendiu;
- b) **Deficiențe de organizare:** utilizarea încorectă sau neadecvată a resurselor IT; folosirea neautorizată a drepturilor de utilizare;
- c) **Greșeli umane:** distrugerea din neglijență a unor echipamente sau a unor date; nerespectarea măsurilor de securitate; defecțiuni datorate acțiunilor improprii ale personalului de întreținere sau intervenție; administrarea necorespunzătoare a sistemului de securitate implementat; organizarea defectuoasă a gestionării informațiilor și datelor;

- d) **Defecțiuni tehnice:** indisponibilitatea surselor de alimentare cu energie electrică; parametri impropri ai energiei electrice; nefuncționarea sisteme de stocare/ înregistrare a datelor; existența unor vulnerabilități ale programelor folosite; acces impropriu la mecanismul tehnic de gestiune a securității informaționale;
- e) **Acte deliberate:** manipularea sau distrugerea echipamentului de protecție a rețelei sau a accesoriilor sale; manipularea frauduloasă a datelor sau a programelor informatice; furt; interceptarea canalelor și liniilor de date ale infrastructurii; accesarea și/sau modificarea neautorizată a sistemului de protecție al rețelei; încercarea sistematică de descoperire a parolilor de acces; utilizarea abuzivă a drepturilor de utilizator; limitarea sau blocarea drepturilor de administrare; facilitarea pătrunderii de viruși/troiieni informatici în rețea; furtul de identitate și accesarea astfel a unor drepturi pentru care nu există autorizare; urmărirea traficului de date; blocarea prin diverse metode a unor servicii sau porturi de date.

5.2.3 Reguli de utilizare corectă a resurselor informatice

- a) Utilizatorii trebuie să anunțe SCTI în cazul în care se observă orice problemă sau breșă în sistemul de securitate al USV cât și orice posibilă întrebuintare greșită sau încălcare a regulamentului în vigoare.
- b) Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip din sistem.
- c) Utilizatorii nu trebuie să încerce să obțină acces la date sau programe pentru care nu au autorizație sau consimțământ explicit.
- d) Utilizatorii nu trebuie să divulge sau să înstrăineze datele de autentificare proprii (nume de cont-uri, parole etc.) utilizate în scopuri de autorizare și identificare în rețeaua informațională a instituției.
- 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 SCTI dacă se consideră necesar.
- g) Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de penetrare a unor restricții de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității sistemului informatic al instituției.
- h) Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care instituția le poate considera ofensive, indecente sau obscene.
- i) Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor USV folosind resursele informatice.

5.2.4 Accesul fizic: toate încăperile în care sunt instalate echipamente ale sistemului informatic trebuie să fie protejate la accesarea fizică neautorizată, în funcție de importanța acestora și tipul datelor vehiculate sau stocate.

5.2.5 Confidențialitatea serviciilor informatice

- a) În scopul administrării sistemului informatic și pentru asigurarea securității acestuia personalul autorizat poate monitoriza activitatea din rețeaua de date cu respectarea confidențialității, în conformitate cu legile în vigoare.
- b) Utilizatorii trebuie să informeze SCTI în legătură cu eventualele suspiciuni de încălcare a confidențialității și să ofere, dacă este posibil, informațiile necesare pentru identificarea problemei.
- c) Confidențialitatea informațiilor transmise prin intermediul resurselor de comunicare ale terților nu poate fi asigurată implicit. Pentru astfel de situații, asigurarea confidențialității și integrității informațiilor sensibile este o obligație a utilizatorilor și are la baza folosirea tehnicilor de securizare (criptare, conexiuni VPN).

5.2.6 Configurarea parametrilor de acces la rețea

- a) Rețeaua informatică a USV este administrată de către SCTI care este responsabil cu întreținerea și dezvoltarea acesteia.
 - b) Toate echipamentele conectate la rețea vor fi configurate conform specificațiilor SCTI.
 - c) Rețeaua locală USV este de tip Ethernet și suportă un set de protocoale de comunicație de rețea în conformitate cu scopul și misiunea instituției.
 - d) Adresele de rețea sunt gestionate centralizat exclusiv de către SCTI
 - e) Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile rețelei USV; este interzisă instalarea de echipamente (*router, switch, hub* sau punct de acces) în rețeaua Intranet USV fără avizul SCTI.
- 5.2.7 Monitorizarea resurselor informatice
- a) Monitorizarea rețelei se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice și a situațiilor de încălcare a regulamentelor de securitate.
 - b) Fișierele jurnal vor fi stocate și vor fi examinate regulat în vederea detectării eventualelor atacuri informatice și abateri de la regulamentele de securitate ale instituției. În această categorie intră următoarele (fără a se limita doar la acestea):
 1. Jurnale ale activității conturilor utilizator;
 2. Jurnale ale scanărilor rețea;
 3. Jurnale ale aplicațiilor;
 4. Jurnale ale solicitărilor de suport tehnic;
 5. Jurnale ale erorilor din sisteme și servere.
- 5.2.8 Securitatea serverelor
- a) Un server nu trebuie conectat la rețeaua instituției 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 *patch*-urilor furnizate de producător;
 3. înlăturarea programelor, a serviciilor sistem și a driverelor care nu sunt necesare;
 4. setarea/activarea parametrilor de securitate, a protecțiilor pentru fișiere și activarea jurnalelor de monitorizare;
 5. dezactivarea sau schimbarea parolelor predefinite;
 6. securizarea accesului la servicii din Internet;
 7. securizarea accesului fizic la echipamente.
- 5.2.9 Parole de acces
- a) Toate parolele trebuie să îndeplinească următoarele condiții:
 1. Să fie schimbate de utilizator în mod regulat;
 2. Să aibă o lungime, în număr de caractere, cât mai mare;
 3. Să aibă diversitate cât mai mare ca și caractere utilizate;
 4. Reutilizarea parolelor este interzisă;
 5. Parolele stocate trebuie securizate;
 6. Parolele de cont utilizator nu trebuie divulgate către terți sub nici o formă, fără excepție;
 - b) Dacă se suspectează că o parolă 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;
 - e) Procedurile de schimbare a parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:
 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.

5.2.10 Recomandări generale pentru alegerea parolelor:

- a) Parolele trebuie să fie schimbate după cel mult 6 luni de utilizare;
- b) Parolele trebuie să aibă o lungime minimă recomandată de 9 caractere;
- c) Parolele trebuie să conțină o varietate cât mai mare de caractere (litere mici și mari, caractere numerice și caractere speciale acolo unde sistemul permite).
- d) Parolele trebuie să respecte următoarele condiții:
 1. nu trebuie să coincidă sau să fie asemănătoare cu numele de utilizator (*login-ul*);
 2. nu trebuie să coincidă sau să fie asemănătoare cu numele utilizatorului;
 3. nu trebuie să coincidă cu date personale (codul numeric personal, data nașterii; numele străzii/orașului; numărul de telefon etc.)
 4. parolele trebuie tratate ca informație confidențială și nu trebuie divulgate în nici o situație.

5.2.11 Sistemul de mesagerie electronică

- a) Următoarele activități sunt interzise:
 1. trimiterea de mesaje cu caracter de intimidare sau hărțuire;
 2. folosirea sistemului de mesagerie electronică în alte scopuri decât cele profesionale;
 3. încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
 4. folosirea altei identități decât cea reală atunci când se trimite email, exceptând cazurile în care persoana este autorizată administrativ în acest scop;
 5. folosirea programelor de poștă electronică neautorizate.
- b) Următoarele activități asociate comunicațiilor de grup sunt interzise deoarece împiedică buna funcționare a rețelei și reduce eficiența comunicărilor electronice:
 1. trimiterea sau retrimiteră email-urilor în lanț;
 2. trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deserveșc instituția;
 3. trimiterea mesajelor de dimensiuni foarte mari;
 4. trimiterea sau retrimiteră mesajelor identificate ca fiind suspecte și care ar putea conține viruși;

5.2.12 Instruire și informare

- a) Informarea angajaților 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 angajaților cu privire la riscurile care conduc la o utilizare necorespunzătoare, intenționată sau neintenționată. Angajații trebuie să cunoască, care sunt amenințările, cum pot fi eliminate riscurile, eventualele probleme legale generate de utilizările necorespunzătoare.

5.2.13 Monitorizare

- a) activitățile utilizatorilor în cadrul rețelei de date și care implică accesul și/sau folosirea sistemului informatic al USV pot fi înregistrate și analizate.
- b) înregistrările activităților de utilizare a sistemului informatic al USV sunt folosite exclusiv în scopul identificării acțiunilor ilegale sau abuzive și respectă criteriile de confidențialitate instituțională și personală.

5.3 Măsuri și reguli pentru asigurarea securității sistemului informatic

5.3.1 Măsuri generale de securitate:

- a) asigurarea alimentării sigure cu energie electrică folosind surse de alimentare neîntreruptibile;
- b) realizarea de verificări și revizii tehnice periodice;

- c) interzicerea utilizării de programe neautorizate;
- d) utilizarea de parole conforme și schimbarea periodică a acestora;
- e) identificarea permanentă a vulnerabilităților sistemelor de protecție; verificarea periodică a nivelului de securitate a rețelei (audit de securitate informațională);
- f) educarea personalului în legătură cu măsurile de securitate necesare și instruirea acestuia pentru utilizarea de programe specifice;
- g) verificarea periodică a sistemelor cu ajutorul programelor anti-virus și asigurarea actualizării permanente a listelor cu definițiile virușilor;
- h) autentificarea în rețea trebuie asigurată numai prin conexiuni de date securizate;
- i) gestiunea corectă a copiilor de rezervă (*back-up*) în ceea ce privește securitatea, integritatea și disponibilitatea acestora prin verificarea permanentă a funcționalității mediilor de păstrare a datelor și a ne-alterării conținutului;

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

- a) utilizatorii rețelei 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 operațiunea de copiere iar acesta va fi păstrat într-un loc sigur;
- b) utilizatorii pot solicita instruirea pentru folosirea în siguranță a stației de lucru și pentru deprinderea modalităților de salvare periodică a datelor de interes;
- c) utilizatorii sistemelor vor urmări actualizarea periodică a sistemului de operare, a programului antivirus instalat precum și actualizarea altor aplicații software utilizate, dacă este cazul;
- d) utilizatorii nu vor instala pe stațiile pe care lucrează programe neautorizate, programe fără licență sau pentru care nu există drepturi legale de utilizare sau aplicații care nu au legătură cu activitatea profesională desfășurată în cadrul instituției;
- e) utilizatorii vor folosi pentru transmiterea/primirea de mesaje electronice de serviciu adresele email instituționale definite în domeniile/subdomeniile administrate de universitate (ex: [utilizator@\[subdomeniu\].usv.ro](mailto:utilizator@[subdomeniu].usv.ro), [utilizator@\[subdomeniu\].usm.ro](mailto:utilizator@[subdomeniu].usm.ro));
- f) Se va evita utilizarea memoriilor externe de tip *flash* (*stick* de date) pentru a reduce expunerea la viruși informatici atât a stației proprii de lucru cât și a rețelei USV;
- g) Atunci când este posibil utilizatorul va verifica credibilitatea sursei unui mesaj email și va investiga formal autenticitatea acestuia evitând deschiderea fișierelor atașate suspecte;

5.3.3 Utilizarea dispozitivelor conectate la rețea (rutere 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) opțiunile de tip *remote management* trebuie să fie limitate la strictul necesar pentru administrare.

5.3.4 Reguli de securitate și conectare la rețeaua wireless:

- a) accesul wireless în rețeaua USV se realizează în mod obișnuit prin autentificare;
- b) în condiții bine definite este posibil accesul public de tip *guest*;
- c) este recomandată evitarea utilizării conexiunilor ne-criptate;
- d) *router-ele* instalate în spațiile USV trebuie să fie configurate și securizate conform recomandărilor SCTI; este interzisă conectarea *router*-elor sau punctelor de acces fără avizul SCTI;
- e) *router-ele* și punctele de acces altele decât cele administrate de SCTI și destinate accesului public cu/fără autentificare vor fi definite (SSID) într-o manieră care să permită identificarea acestora și a amplasamentului lor fizic (corp clădire, număr sală/birou);

5.3.5 Politica de securitate a dispozitivelor mobile (telefoane, tablete):

- a) sistemul de operare și aplicațiile 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 rețeaua wireless usw.

5.4 Monitorizarea eficienței rețelei informatice

5.4.1 Protecția eficientă a rețelei informatice a instituției conduce la creșterea indicatorilor de performanță asociați utilizării acesteia și la îmbunătățirea gradului de satisfacție al beneficiarilor direcți.

Indicatori urmăriți:

- a) eficiența accesului la resurse electronice de informare, comunicare electronică și transfer de date;
- b) nivelul de performanță al echipamentelor de comunicație și al infrastructurii de date;
- c) gradul de creștere a operativității îndeplinirii sarcinilor de către salariați;
- d) gradul de diminuare a timpului necesar elaborării documentelor standard;
- e) gradul de creștere a operativității în furnizarea de informații sau documente către solicitanți;
- f) nivelul general de satisfacție al utilizatorilor rețelei de date USV.

6. RESPONSABILITĂȚI

6.1 **Coordonatorul SCTI** are următoarele responsabilități și competențe:

- a) creează condițiile de aplicare a prezentei procedurii;
- b) monitorizează nivelul de securitate informațională și propune măsuri de optimizare;
- c) numește responsabili care să asigure elaborarea / modificarea și gestionarea procedurilor specifice în cadrul serviciului;

6.2 **Oficiul Juridic** are următoarele responsabilități și competențe:

- a) aduce la cunoștința conducerii compartimentelor apariția / modificarea actelor care reglementează sau legiferează activitățile specifice;

7. DISPOZIȚII FINALE

7.1 Aprobarea modificării prezentei proceduri este de competența Senatului USV.

7.2 Prezenta procedură intră în vigoare din momentul aprobării în Senatul USV.

7.3 Verificarea modului în care se aplică prezenta procedură se realizează de Directorul General Administrativ.

7.4 Prezenta abrogă ediția precedentă a procedurii aprobat prin hotărârea nr. _____ în ședința de Senat din _____.

8. ANEXE

Lista anexelor care însoțesc această procedură este redată după cum urmează:

	Denumire	Cod
Anexa 1	Listă de difuzare / retragere a documentelor	PO-SCTI-01 F01
Anexa 2	Lista parolelor alocate – strict confidențial 1 ex se păstrează la Director SCTI.	PO-SCTI-01 F02

Anexa 1.

Listă de difuzare / retragere a documentelor
PO-SCTI-01 F01

Listă de difuzare nr.	1	Denumire document difuzat, cod	Anexa 2 - PO-CIC-01 F02
-----------------------	---	--------------------------------	-------------------------

Nr. ex.	Difuzare			Data retragerii	Observații
	Numele și prenumele	Data	Semnătura		
1.	Buta Marius				
2.	Balan Doru				
3.	Gheorghiu Florin				
4.	Creangă Cristi				
5.	Cunițchi Stelian				
6.	Coțovanu Sebastian				
7.	Andrieș Marian				
8.	Gordin Ionel				
9.	Ovadiuc Ana-Maria				
10.	Maciuc Ovidiu				
11.	Vultur Oana				

	Numele și prenumele	Semnătura
Elaborat	Vultur. Oana	