Universitatea
Ştefan cel Mare
Suceava

HOTĂRÂREA
Consiliului de Administraţie al Universităţii „Ştefan cel Mare" din Suceava
Nr. **6** din data de **17 ianuarie 2017**

cu privire la aprobarea Procedurii operaţionale privind securitatea informaţiilor şi a sistemului IT (PO-SCTI-03)

În conformitate cu prevederile O.U.G. nr. 1 din data de 04.01.2017 pentru stabilirea unor măsuri în domeniul administraţiei publice centrale şi pentru modificarea şi completarea unor acte normative;

Având în vedere discutarea şi aprobarea în cadrul Şedinţei Consiliului de Administraţie din data de 17.01.2016 a propunerii de aprobare a Procedurii operaţionale privind securitatea informaţiilor şi a sistemului IT , în cadrul Universităţii „Ştefan cel Mare" din Suceava;

În conformitate cu prevederile Legii Educaţiei Naţionale nr.1/2011 cu modificările şi completările ulterioare;

În baza art.53 din Carta Universităţii „Ştefan cel Mare" din Suceava, Consiliul de Administraţie al USV hotărăşte:

Art. 1. Se aprobă Procedura operaţională privind securitatea informaţiilor şi a sistemului IT (PO-SCTI-03).

Art. 2. Serviciul de comunicaţii şi tehnologii informaţionale va duce la îndeplinire dispoziţiile prezentei hotărâri.

Preşedintele Consiliului de Administraţie,
Rector,
Prof.univ.dr.ing. Valentin POPA

ROMÂNIA MINISTERUL EDUCAŢIEI NAŢIONALE ŞI CERCETĂRII ŞTIINŢIFICE USV Universitatea Ştefan cel Mare din Suceava

Vizat,
Consilier Juridic Oana BOICU POSAŞTIUC

V.P./A.N./1ex.

Cuprins

1. SCOPUL PROCEDURII

Procedura stabileşte politicile, principiile şi modalităţile de acţiune pentru asigurării securităţii informaţiilor şi a sistemului IT din Universitatea „Ştefan cel Mare" din Suceava.

2. DOMENIUL DE APLICARE

Procedura se aplică în cadrul Serviciului de Comunicaţii şi Tehnologii Informaţionale din Universitatea Ştefan cel Mare din Suceava

3. DOCUMENTE DE REFERINŢĂ

3.1. Reglementări internaţionale

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 Convenţia privind criminalitatea informatică - Monitorul Oficial, Partea I nr. 343 din 20/04/2004
3.3.4 Declaraţia privind libertatea comunicării pe Internet adoptată la Strasbourg în 2003

3.2. Legislaţie primară

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

3.3. Legislaţie secundară

3.3.1 Norma tehnică şi 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 autorităţile şi instituţiile administraţiei publice centrale şi locale

4. DEFINIŢII ŞI ABREVIERI

4.1 Termeni şi definiţii

4.1.1 **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.
4.1.2 **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.

Spre deosebire de un virus informatic, un vierme nu are nevoie să se ataşeze la anumite fişiere 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 retea a unor fisiere 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 informaţii 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 fişierele. De obicei pentru deblocarea sistemului şi/sau recuperarea fişierelor se solicită plaţi în scopul declarat de furnizare ulterioara a cheilor de decriptare, neexistând însă nicio garanţie 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 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 cu sau fără ştiinţa sau intenţia utilizatorului.

4.1.7 **Expunere** - Reducerea a constrângerilor impuse pentru accesarea informaţiilor.

4.1.8 **Vulnerabilitate** - Slăbiciune care poate fi exploatată în scopul accesării neautorizate a resurselor sau informaţiilor.

4.1.9 **Atac** - Încercarea de a exploata vulnerabilitatea.

4.1.10 **Control** - Măsură de gestionare vulnerabilităţii de obicei in scopul reducerii expunerii la riscuri.

4.2 Abrevieri

USV	– Universitatea Ştefan cel Mare din Suceava
SCTI	– Serviciul de Comunicaţii şi Tehnologii Informaţionale

5. CONŢINUT

5.1 Principiile asigurării securităţii informaţionale

5.1.1 Principiile care trebuie îndeplinite pentru a asigura securitatea sistemelor informatice sunt:

a) **Principiul responsabilităţii.** Responsabilităţile legate de securitate informaţională pentru deţinători, furnizori şi utilizatori de sisteme informatice sau servicii de date trebuie să fie explicite.

b) **Principiul conştientizării.** Pentru a asigura securitatea sistemelor informatice, deţinătorii, furnizorii şi utilizatorii acestora trebuie să poată accesa şi dobândi cunoştinţele necesare, să fie informaţi despre existenţa şi cadrul general al măsurilor, practicilor şi procedurilor de securitate a sistemelor informatice şi să poată acţiona voluntar pentru reducerea riscurilor.

c) **Principiul eticii.** Sistemele informatice şi securitatea sistemelor informatice trebuie folosite într-o manieră în care drepturile şi interesele legale ale celorlalţi să nu fie afectate.

d) **Principiul multidisciplinarităţii.** Măsurile, practicile şi procedurile de asigurare a securităţii sistemelor informatice trebuie să ţină cont de toate consideraţiile şi aspectele

relevante, inclusiv tehnice, administrative, organizaţionale, operaţionale, comerciale, educaţionale şi legale.

e) **Principiul proporţionalităţii.** Nivelurile de securitate, costurile, măsurile, practicile şi procedurile trebuie să fie corespunzător dimensionate şi proporţionale cu valoarea şi gradul de încredere necesar pentru fiecare tip de informaţie avându-se în vedere de asemenea şi nivelul daunelor potenţiale respectiv probabilitatea de apariţie a acestora.

f) **Principiul integrării.** Măsurile, practicile şi procedeele de asigurare a securităţii sistemelor informatice trebuie să fie coordonate instituţional şi integrate şi cu alte măsuri, practici şi procedee ale organizaţiei cu scopul creării unui sistem global de securitate informaţională coerent.

g) **Principiul actualităţii.** Instituţiile, indiferent de tipul lor, trebuie să acţioneze rapid şi într-o manieră coordonată pentru a preveni şi a răspunde eficient la apariţia breşelor de securitate a sistemelor informatice.

h) **Principiul reevaluării.** Securitatea sistemelor informatice trebuie analizată şi reevaluată periodic pentru a răspunde celor mai noi tipuri de agresiuni informatice.

i) **Principiul democraţiei.** Securitatea sistemelor informatice trebuie să nu restrângă drepturile de utilizare legitimă a reţelelor de date.

5.1.2 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, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul USV, 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 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 daunele ce pot fi produse ca urmare a nefuncţionării lor corespunzătoare. Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor şi procedurilor de securitate. Acestea sunt obligatorii pentru toţi utilizatorii resurselor informatice.

5.2 Politica de securitate în utilizarea resurselor informatice din cadrul USV

5.2.1 Scopul elaborării politicii de securitate informaţională

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

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

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

5.2.2 La întocmirea planului 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 intervenţie; administrarea necorespunzătoare a sistemului de securitate implementat; organizarea defectuoasă a gestionării informaţiilor şi datelor;

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

e) **Acte deliberate**: manipularea sau distrugerea echipamentului de protecţie a reţelei sau a accesoriilor sale; manipularea frauduloasa a datelor sau a programelor informatice; furt; interceptarea canalelor şi liniilor de date ale infrastructurii; accesarea si/sau modificarea neautorizată a sistemului de protecţie al 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 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 anunţe SCTI în cazul în care se observă orice problemă sau breşă în sistemul de securitate al USV cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentului în vigoare.

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 cont-uri, 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* sa se faca cu responsabilitate, eventual cu consultarea SCTI dacă se consideră necesar.

g) Utilizatorii nu trebuie să descarce, 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 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 funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.

5.2.5 Confidenţialitatea 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 SCTI 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 baza folosirea tehnicilor de securizare (criptare, conexiuni VPN).

5.2.6 Configurarea parametrilor de acces la reţea

a) Reţeaua informatică a USV este administrată de către SCTI care este responsabil cu întreţinerea şi dezvoltarea acesteia.
b) Toate echipamentele conectate la reţea vor fi configurate conform specificaţiilor SCTI.
c) Reţeaua locală USV este de tip Ethernet si 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 SCTI
e) Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei USV; este interzisă instalarea de echipamente (*router*, *switch*, *hub* sau punct de acces) în reţeaua Intranet USV fără avizul SCTI.

5.2.7 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 abateri de la regulamentele de securitate ale instituţiei. În această categorie intră următoarele (fără a se limita doar la acestea):
   1. Jurnale ale activităţii conturilor utilizator;
   2. Jurnale ale scanărilor reţea;
   3. Jurnale ale aplicaţiilor;
   4. Jurnale ale solicitărilor de suport tehnic;
   5. Jurnale ale erorilor din sisteme şi servere.

5.2.8 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 *patch*-urilor furnizate de producător;
   3. înlăturarea programelor, a serviciilor sistem şi a driverelor care nu sunt necesare;
   4. setarea/activarea 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.

5.2.9 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, in număr de caractere, cat mai mare;
   3. Să aba diversitate cat 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 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 conţină o varietate cat mai mare de caractere (litere mici şi mari, caractere numerice şi caractere speciale acolo unde sistemul permite).
   d) Parolele trebuie să respecte următoarele condiţii:
      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 naşterii; numele străzii/oraşului; numărul de telefon etc.)
      4. parolele trebuie tratate ca informaţie confidenţială şi nu trebuie divulgate în nici o situaţie.

5.2.11 Sistemul de mesagerie electronică
   a) Următoarele activităţi sunt interzise:
      1. trimiterea de mesaje cu caracter de intimidare sau hărţuire;
      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 identităţi decât cea reală atunci când se trimite email, exceptând cazurile în care persoana este autorizată administrativ în acest scop;
      5. folosirea programelor de poştă electronică neautorizate.
   b) Următoarele activităţi asociate comunicaţiilor de grup sunt interzise deoarece împiedică buna funcţionare a reţelei şi reduce eficienţa comunicărilor electronice:
      1. trimiterea sau retrimiterea email-urilor în lanţ;
      2. trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia;
      3. trimiterea mesajelor de dimensiuni foarte mari;
      4. trimiterea sau retrimiterea mesajelor identificate ca fiind suspecte şi care ar putea conţine viruşi;

5.2.12 Instruire şi 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.

5.2.13 Monitorizare
   a) activităţile utilizatorilor în cadrul reţelei de date şi care implică accesul şi/sau folosirea sistemului informatic al USV pot fi înregistrate şi analizate.
   b) înregistrările activităţilor de utilizare a sistemului informatic al USV sunt folosite exclusiv în scopul identificării acţiunilor ilegale sau abuzive şi respectă criteriile de confidenţialitate instituţională şi personală.

5.3 Măsuri şi reguli pentru asigurarea securităţii sistemului informatic

5.3.1 Măsuri generale de securitate:
   a) asigurarea alimentării sigure cu energie electrica 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; verificarea periodică a nivelului de securitate a reţelei (audit de securitate informaţională);
f) educarea personalului în legătură cu măsurile de securitate necesare şi instruirea acestuia pentru utilizarea de programe specifice;
g) verificarea periodică a sistemelor cu ajutorul programelor anti-virus şi asigurarea actualizării permanente a listelor cu definiţiile virusilor;
h) autentificarea în reţea trebuie asigurată numai prin conexiuni de date securizate;
i) gestiunea corecta 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 ne-alterării conţinutului;

5.3.2 Reguli de bază pentru utilizatorii individuali ai sistemelor din reţea:
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 intr-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 altor aplicaţii 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 universitate (ex: utilizator@[subdomeniu].usv.ro, utilizator@[subdomeniu].usm.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 USV;
g) Atunci când este posibil utilizatorul va verifica credibilitatea sursei unui mesaj email şi va investiga formal autenticitatea acestuia evitând deschiderea fişierelor ataşate suspecte;

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

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

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

a) sistemul de operare şi aplicaţiile utilizate trebuie sa 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 usv.

5.4 Monitorizarea eficienţei reţelei informatice

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

6. RESPONSABILITĂŢI

6.1 **Coordonatorul SCTI** are următoarele responsabilităţi şi competenţe:

a) creează condiţiile de aplicare a prezentei procedurii;
b) monitorizează nivelul de securitate informaţională şi propune masuri de optimizare;
c) numeşte responsabili care să asigure elaborarea / modificarea şi gestionarea procedurilor specifice în cadrul serviciului;

6.2 **Oficiul Juridic** are următoarele responsabilităţi şi competenţe:

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

7. DISPOZIŢII FINALE

7.1 Aprobarea modificării prezentei proceduri este de competenţa 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 ediţia precedentă a procedurii aprobat prin hotărârea nr. _____ în şedinţa de Senat din _____.

8. ANEXE

Lista anexelor care însoţesc 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 confidenţial 1 ex se păstrază 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	Observaţii
	Numele şi prenumele	Data	Semnătura		
1.	Buta Marius				
2.	Balan Doru				
3.	Gheorghiu Florin				
4.	Creangă Cristi				
5.	Cunitchi Stelian				
6.	Coţovanu Sebastian				
7.	Andrieş Marian				
8.	Gordin Ionel				
9.	Ovadiuc Ana-Maria				
10.	Maciuc Ovidiu				
11.	Vultur Oana				

	Numele şi prenumele	Semnătura
Elaborat	Vultur. Oana	