

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I
		Nr.de ex.: 5
COMISIA	Cod: P.S. 12.02	Revizia: -
		Nr.de ex. :-
		Pagina 1 din 18
		Exemplar nr.: 1

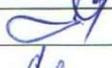
1. Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau după caz, a reviziei în cadrul ediției procedurii de sistem

Nr. Crt.	Elemente privind responsabilii/operatiunea	Numele si prenumele	Functia	Data	Semnatura
	1	2	3	4	5
1.1.	Elaborat	Stanisor Maria Mirabela	Consilier	29.12.2017	
1.2.	Verificat	Bobilca Dan	Vicepresedinte comisie SCIM	29.12.2017	
1.3.	Avizat	Paloiu Daniela	Presedinte Comisie SCIM	29.12.2017	
1.4.	Aprobat	Avan Catalin	Primar	29.12.2017	

2. Situația edițiilor și a reviziilor în cadrul edițiilor procedurii de sistem

Nr. Crt.	Editia/ revizia in cadrul editiei	Componenta revizuita	Modalitatea reviziei	Data de la care se aplica prevederile editiei sau reviziei editiei
	1	2	3	4
2.1.	Editia I	Elaborarea ediției inițiale	Conform ORDIN nr. 400/2015 pentru aprobarea Codului controlului intern managerial al entităților publice	

3. Lista cuprinzând persoanele la care se difuzează ediția sau, după caz, revizia din cadrul ediției procedurii de sistem

Nr. crt.	Scopul difuzarii	Ex. nr.	Compartiment	Functia	Nume si prenume	Data primirii	Semnatura	
0	1	2	3	4	5	6	7	
3.1.	Aplicare	1	Toate compartimentele	Conform Lista de difuzare				
3.2.	Informare	2		Primar	Avan Catalin			
3.3.	Evidenta	3	Comisie SCIM	Secretar comisie	Chitoiu Ana Maria			
3.4.	Control SCIM	4	Comisie SCIM	Presedinte	Paloiu Daniela			
3.5.	Arhivare	5	Arhiva	Responsabil arhiva	Toabes Elena			

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 2 din 18
		Exemplar nr.: 1

4. Scop

Stabilirea unui cadru general privind asigurarea integrității, confidențialității și disponibilității informației în cadrul UATC Pausesti;

Furnizeaza personalului si conducerii un instrument care faciliteaza gestionarea riscurilor privind asigurarea integrității, confidențialității și disponibilității informației într-un mod controlat si eficient, pentru atingerea obiectivelor prestabilite, atat a celor generale cat si specifice.

Furnizeaza o descriere a modului in care sunt stabilite si implementate actiunile/masurile de control menite sa previna aparitia riscurilor.

5. Domeniu de aplicare

Procedura se aplica in cadrul UATC Pausesti in toate structurile in vederea gestionarii riscurilor privind asigurarea integrității, confidențialității și disponibilității informației .

6. Documente de referință aplicabile activitatii procedurale

6.1. Legislatie primara:

LEGEA Nr. 544 din 12.10.2001 privind liberul acces la informațiile de interes public.

Legea 215 din 23.04.2001 – privind administrația publică locală, republicată;

Legea 161 din 19.05.2003 privind asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice si în mediul de afaceri, prevenirea si sancționarea corupției;

Legea nr. 455 din 2001 privind semnatura electronică-republicata;

Legea nr.8 din 14 martie 1996 privind dreptul de autor și drepturile conexe

Legea Nr.506 din 17.11.2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

Legea Nr.52 din 21.01.2003 privind transparența decizională în administrația publică

O.U.G. Nr. 79 din 13 iunie 2002, privind cadrul general de reglementare a comunicațiilor;

6.2. Legislatie secundara

Ordinul M.A.P. 252 din 02.06.2003 – pentru aprobarea Normelor metodologice privind instruirea si specializarea în domeniul informaticii a functionarilor publici;

Hotărârea 1007 din 04.10.2001 pentru aprobarea Strategiei Guvernului privind informatizarea Administrației Publice;

Hotărârea nr. 1440 din 12.12.2002 privind aprobarea Strategiei naționale pentru promovarea noii economii si implementarea societății informaționale;

Ordinul Avocatului Poporului Nr.52 din 18.04.2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.

Ordinul Secretariatului General al Guvernului nr.400/2015 pentru aprobarea Codului controlului intern/managerial al entitatilor publice.

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 3 din 18
		Exemplar nr.: 1

7. Definitii si abrevieri

7.1. Definitii:

Resurse Informatice și de Comunicații (RIC): toate dispozitivele de tipărire/imprimare, dispozitive de afișare, unități de stocare, și toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (notebook-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant - PDA*), pagere, sisteme de procesare distribuită, echipament de laborator și medical conectat la rețea și controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante și alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele și datele care sunt proiectate, construite, puse în funcțiune (operaționale) și menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afișa și transmite informația.

Administratorul Resurselor Informatice și de Comunicații: Responsabil la nivelul Institutiei publice cu administrarea și finanțarea RIC. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea și aprobarea regulamentelor privind activitățile de finanțare, administrare și utilizare a RIC. Titlul este atribuit în mod automat ordonatorului de credite, adică primarului.

Responsabil cu Securitatea RIC (RSRIC): Răspunde direct doar în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Institutiei publice. Este persoana de contact intern și extern a Institutiei publice pentru orice problemă în legătură cu securitatea RIC. Funcția RSRIC este atribuită administratorului de rețea (responsabilului IT din cadrul instituției).

Responsabil cu securitatea RIC la nivel de compartiment (RSRICC): Persoana responsabilă de monitorizarea și implementarea controalelor de securitate și a procedurilor pentru sistemul RIC la nivelul unui compartiment. Funcția RSRICC este atribuită șefului de serviciu, birou, compartiment.

Utilizator: O persoană, o aplicație automatizată sau proces utilizator autorizat de către Institutia publica, în conformitate cu procedurile și regulamentele în vigoare, să folosească resursele informatice și de comunicații.

Abuz de privilegii: Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Institutiei publice și/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înlăptuirea de către utilizator a acțiunii respective.

Furnizor: Persoană fizică/juridică care oferă bunuri și/sau servicii Institutiei publice în baza unui contract comercial sau de colaborare.

Internet: Sistem global care interconectează calculatoare și rețele de calculatoare. Acestea sunt deținute de mai multe organizații, agenții guvernamentale, societăți, instituții academice.

Intranet: Rețea privată destinată comunicațiilor și partajării informațiilor, care, ca și rețeaua Internet, folosește suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizați din cadrul unei organizații (instituții). În mod obișnuit, rețeaua Intranet a unei organizații este protejată printr-un sistem de protecție (firewall).

Echipa de Răspuns la Incidentele de Securitate a RIC (ERIS): persoanele responsabile de

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I
		Nr.de ex.: 5
COMISIA	Cod: P.S. 12.02	Revizia: -
		Nr.de ex. :-
		Pagina 4 din 18
		Exemplar nr.: 1

acțiunile desfășurate în scopul micșorării sau eliminării impactului negativ al unui incident de securitate. ERIS este formată din ARIC, RSRIC, RSRICC.

Virus: Un program care se auto-atășează la un fișier executabil sau la o aplicație vulnerabilă și care generează efecte de la cele deranjante până la cele distructive. Un virus se execută în momentul în care este accesat un fișier infectat. Un virus de macro infectează codul executabil încapsulat în pachetul de programe Microsoft Office (Word, Excel, PowerPoint) sau alte programe care permit utilizatorului să genereze macro-uri.

Vierme: Un program care se auto-copiază în oricare altă parte a unui sistem informatic. Aceste copii pot fi create pe același calculator sau pot fi trimise către alte calculatoare prin intermediul rețelei. Prima utilizare a termenului descria un program care s-a multiplicat într-o rețea de calculatoare, folosind resursele sau calculatoarele neutilizate din rețea pentru a distribui aceste copii. Unii dintre acești viermi reprezintă o amenințare la adresa securității datorită faptului că folosesc rețeaua pentru a se împrăști, împotriva voinței proprietarilor de sisteme de calcul, cauzând astfel nefuncționarea sau funcționarea defectuoasă a rețelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferența constând în faptul că un vierme nu are nevoie să se atășeze la anumite fișiere pentru a se multiplica.

Cal troian: de obicei un virus sau un vierme – care este ascuns sub forma unui program atractiv sau inofensiv, cum ar fi un joc, sau program de grafică (o felicitare în format electronic, un program tip screen-saver). Victimele pot primi un astfel de cal troian prin email sau pe o dischetă, adeseori de la o altă victimă necunoscută sau pot fi încurajate să descarce un fișier de pe o pagină Web sau un forum.

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.

Rețea locală (LAN): O rețea de comunicații de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Rețeaua locală oferă comunicații între calculatoare și periferice la o viteză de transfer mare și cu puține erori.

Server: Un program de calculator care oferă servicii altor programe aflate pe același calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe același calculator mai pot rula și alte programe de tip client sau server.

Gazdă (Host): Un sistem care oferă servicii pentru un anumit număr de utilizatori.

Copii de Siguranță (backup): Copii ale fișierelor și aplicațiilor făcute pentru a evita pierderea datelor și pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.

Firewall: Un mecanism de control al accesului care acționează ca o barieră între două sau mai multe segmente ale unei rețele de calculatoare sau ale unei arhitecturi de tip client/server, folosit pentru a proteja rețelele interne sau segmente ale acestora împotriva utilizatorilor sau proceselor neautorizate.

Atac informațional: O încercare de a trece peste măsurile și controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului de resurse informatice și

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 5 din 18
		Exemplar nr.: 1

comunicatii. Atacatorul poate altera informațiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular și de eficacitatea contramăsurilor aplicate.

Protecție informațională: Acțiuni întreprinse în vederea afectării informațiilor și sistemelor informatice ostile, în timp ce protejează informațiile și sistemele informatice proprii.

Procedura - reprezintă modalitatea specifică de desfășurare a unei activități sau a unui proces.

7.2. Abrevieri:

Nr. crt.	Abrevierea	Termenul abreviat
1	P.O.	Procedura operationala
2	E	Elaborare
3	V	Verificare
4	A	Aprobare
5	Ap.	Aplicare
6	Ah.	Arhivare
7	ROF	Regulament de organizare si functionare

8. Descrierea procedurii

8.1. Generalitati

Prezenta procedura este elaborata pentru a stabili un cadru corect, legal și eficient de utilizare a tehnologiei informației și comunicațiilor în Institutia publica. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea acestea au ca scop protejarea imaginii instituției și a investițiilor acesteia pentru dezvoltarea sistemul informatic și de comunicații.

Având în vedere că majoritatea personalului instituției sunt familiarizati cu utilizarea calculatorului se presupune că aceștia sunt familiarizați cu termenii tehnici și de asemenea cunosc sistemul de operare Windows și pachetul de programe Microsoft Office.

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

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 Institutiei publice, sunt proprietatea instituției în condițiile legilor în vigoare. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la sistemul resurselor informatice si de comunicatii.

Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor sistemului resurselor informatice si de comunicatii. Diverse aplicații au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a sistemului resurselor informatice si de comunicatii.

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I
		Nr.de ex.: 5
COMISIA	Cod: P.S. 12.02	Revizia: -
		Nr.de ex. :-
		Pagina 6 din 18
		Exemplar nr.: 1

regulamentelor și procedurilor de securitate. Acestea sunt obligatorii pentru toți utilizatorii sistemului resurselor informatice și de comunicații.

Clasificarea Informațiilor

Clasificarea informațiilor este necesară pentru a permite atât alocarea resurselor necesare protecției acestora cât și pentru a determina pierderile potențiale ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora. Pentru a asigura securitatea și integritatea informațiilor, acestea se împart în trei categorii principale:

- Publice
- Secrete
- Strict Secrete

Persoanele responsabile și conducerea instituției răspund de evaluarea periodică a schemei de clasificare a informațiilor. Toate informațiile din Instituția publică trebuie să se regăsească în una din următoarele categorii:

Publice. Acestea sunt informațiile accesibile oricărui utilizator din interiorul sau exteriorul Instituției publice. Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra Instituției publice sau aceste efecte sunt ne semnificative. Utilizatorii care furnizează aceste informații sunt responsabili de asigurarea integrității și disponibilității acestora în raport cu cerințele Instituției publice.

Secrete. În această categorie se includ informațiile pe care Instituția publică trebuie să le protejeze conform legislației în vigoare. Aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate și distribuite în cadrul Instituției publice doar utilizatorilor autorizați. Distribuirea acestor informații de către utilizatorii autorizați trebuie să se facă pe baza unei clauze de confidențialitate.

Strict Secrete sau Confidențiale. În această categorie se includ toate informațiile care datorită valorii naturii lor nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidența Codului Civil, Penal sau legislației în vigoare. Accesul la aceste informații va fi restricționat. Datele strict secrete nu pot fi copiate, distribuite sau șterse fără acordul scris al conducerii Instituției publice.

Confidențialitate

Fișierele electronice create, trimise, primite sau stocate folosind sistemul de resurse informatice și de comunicații propriu, administrate sau în custodia și sub controlul Instituției publice nu au caracter personal și pot fi accesate oricând de către angajații autorizați (specialistul IT/administrator rețea) fără înștiințarea utilizatorului.

În scopul administrării resurselor informatice și de comunicații și pentru asigurarea securității acestora, personalul autorizat poate revizui sau utiliza orice informație stocată pe sau transportată prin sistemele resurselor informatice și de comunicații în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor.

Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Instituției publice, orice incident de posibilă întrebuintă greșită.

Un mare număr de utilizatori, pot accesa diverse informații din sistemul de comunicații al Instituției publice. În aceste condiții este obligatorie păstrarea confidențialității acestor

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I
		Nr.de ex.: 5
COMISIA	Cod: P.S. 12.02	Revizia: -
		Nr.de ex. :-
		Pagina 7 din 18
		Exemplar nr.: 1

informațiilor transmise din exteriorul resurselor informatice și de comunicații și a informațiilor obținute din interior.

Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele Institutiei publice pentru care nu au autorizație sau consimțământ explicit.

Nici un utilizator al sistemului de resurse informatice și de comunicații ale Institutiei publice nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemului resurselor informatice și de comunicații. Această regulă se extinde și după ce utilizatorul a încheiat relațiile cu Institutia publică, conform angajamentelor personale sau contractelor de munca semnate, existente în cadrul Serviciului Resurse Umane.

Confidențialitatea informațiilor transmise prin intermediul resurselor de comunicații ale terților nu poate fi asigurată. Pentru aceste situații, confidențialitatea și integritatea informațiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligați să se asigure că toate informațiile confidențiale ale Institutiei publice se transmit în așa fel încât să se asigure confidențialitatea și integritatea acestora.

8.2. ADMINISTRAREA RESURSELOR INFORMATICE SI DE COMUNICATII

8.2.1 Accesul Administrativ

Utilizatorii trebuie să cunoască și să accepte toate aspectele privind securitatea resurselor informatice și de comunicații înainte de a li se permite accesul la un cont.

Utilizatorii care au conturi de acces administrativ trebuie să aibă instrucțiuni de administrare, documentare, instruire și autorizare a conturilor. Aceste instrucțiuni se vor elabora de către fiecare compartiment și vor fi incluse în fișa postului.

Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al responsabilului IT și trebuie să fie schimbată atunci când o persoană care utilizează acest cont își schimbă locul de muncă din cadrul compartimentului sau a Instituției, sau în cazul unei modificări a listei de personal ale terților (furnizor desemnat) în contractele cu primăria .

Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operațiuni definite. Acestea trebuie să îndeplinească următoarele condiții:

- trebuie să fie autorizate;
- trebuie create cu dată de expirare specifică;
- contul va fi șters atunci când nu mai este necesar.

8.2.2. Accesul Fizic

Accesul fizic la toate încăperile în care sunt instalate resurse informatice și de comunicații trebuie să fie documentat și monitorizat.

Toate încăperile în care sunt instalate resurse informatice și de comunicații trebuie să fie protejate fizic, în funcție de importanța acestora și tipul datelor vehiculate sau stocate.

Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului de resurse informatice și de comunicații se aprobă accesul doar pentru personalul care răspunde de buna funcționare a echipamentelor din încăperea respectivă și, dacă este cazul, părților contractante, ale căror obligații contractuale implică acces fizic.

Personalul care are drepturi de acces trebuie să dețină legitimație de serviciu și acte de identitate care să-i ateste calitatea. Nu este permis transferul dreptului de acces indiferent de motiv.

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 8 din 18
		Exemplar nr.: 1

Accesul publicului, vizitatorilor, sau a persoanelor străine în cadrul instituției se va face doar pe baza actului de identitate. Vizitatorii/persoanele străine trebuie să fie însoțiți în zonele cu acces restricționat.

8.2.3. Configurarea Parametrilor de Acces la Rețea

Infrastructura de comunicații, rețeaua de comunicații digitale, a Primăriei Pausesti este administrată de către Compartimentul IT care este responsabil cu întreținerea și dezvoltarea acesteia.

Pentru a furniza o infrastructură de comunicații unitară cu posibilități de modernizare toate componentele acesteia sunt instalate de către Compartimentul IT sau de către un furnizor avizat explicit de către Compartimentul IT.

Toate echipamentele, fără excepție, conectate la rețeaua de comunicații trebuie configurate conform specificațiilor Compartimentul IT

Orice dispozitiv hardware, inclusiv plăcile de rețea și modemuri, care se va conecta la rețeaua primăriei, trebuie să fie însoțit de o aprobare de tip (producător, model etc.) din partea Compartimentul IT.

Modificarea configurației oricărui dispozitiv activ conectat la rețeaua de comunicații se face numai de către Compartimentul IT.

Adresele de rețea sunt alocate dinamic sau static numai de către Compartimentul IT.

Toate conectările dintre rețeaua de comunicații a primăriei și alte rețele de comunicații, publice sau private, sunt responsabilitatea exclusivă a Compartimentul IT

Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile rețelei (este interzisă instalarea unui telefon, fax, modem, router, switch, hub sau punct de acces la rețeaua Instituției) fără aprobare din partea Compartimentul IT. Utilizatorilor li se interzice instalarea de dispozitive hardware de rețea sau programe care furnizează servicii de rețea fără aprobarea Compartimentul IT.

8.2.4. Tratarea Incidentelor de Securitate

Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activități suspecte, informații modificate etc., trebuie urmate procedurile standard specifice pentru micșorarea riscurilor.

Responsabilul IT este responsabil cu strângerea dovezilor fizice și electronice ce vor face parte din documentația pentru tratarea incidentului.

Folosind resurse tehnice speciale se va monitoriza nivelul daunelor și gradul de eliminare sau atenuare a vulnerabilităților acolo unde este cazul.

În cazul în care incidentul nu implică acțiuni contrare legilor în vigoare Responsabilul IT va recomanda conducerii entității sancțiuni disciplinare.

În cazul în care incidentul implică aplicarea legilor civile sau penale Responsabilul IT va recomanda conducerii entității sesizarea organelor în drept ale statului.

8.2.5. Monitorizarea Resurselor Informatice și de Comunicații

Monitorizarea resurselor informatice și de comunicații se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice și a situațiilor de încălcare a normelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări și înregistra:

- Tipul traficului (ex. structura pe protocoale și servicii) extern și conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
- Tipul traficului în rețea, a protocoalelor și a echipamentelor conectate la resurse

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 9 din 18
		Exemplar nr.: 1

informatice si de comunicatii, conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.

- Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

Fișierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice și abateri de la normele de securitate ale entității. În această categorie intră următoarele (fără a se limita doar la acestea):

- Jurnale ale sistemelor de detectarea automată a intrușilor.
- Jurnale Firewall
- Jurnale ale activității conturilor utilizator
- Jurnale ale scanărilor rețea
- Jurnale ale aplicațiilor
- Jurnale ale erorilor din sisteme și servere.

8.2.6. Securitatea Serverelor

Un server nu trebuie conectat la rețeaua primăriei până când nu se află într-o stare sigură acreditată de către Responsabilul IT.

Procedura de securizare a serverelor trebuie să includă obligatoriu următoarele:

- Instalarea sistemului de operare dintr-o sursă aprobată
- aplicarea patch-urilor furnizate de producător
- înlăturarea programelor, a serviciilor sistem și a driver-ilor care nu sunt necesare
- setarea/activarea parametrilor de securitate, a protecțiilor pentru fișiere și activarea jurnalelor de monitorizare
- dezactivarea sau schimbarea parolelor conturilor predefinite
- securizarea accesului fizic la aceste echipamente

Compartimentul IT va monitoriza obligatoriu pentru serverele principale (enterprise) procesul de instalare și aplicare regulată a patch-urilor de securitate și, prin sondaj, pentru serverele departamentale sau a grupurilor de lucru.

8.2.7. Crearea și Utilizarea Copiilor de Siguranță (Backup)

Frecvența, dimensiunea și conținutul copiilor de siguranță trebuie să fie în concordanță cu importanța informației și cu riscul acceptat de proprietarul datelor.

Procedura standard de creare a copiilor de siguranță și de recuperare pentru fiecare sistem din cadrul resurselor informatice si de comunicatii trebuie să fie documentată și periodic revizuită. Verificarea copiilor de siguranță se va face după o procedură documentată și revizuită periodic.

Copiile de siguranță trebuie să fie periodic testate pentru a asigura faptul că informațiile stocate sunt recuperabile.

Accesul la mediile de backup ale Primăriei se va face numai de personalul abilitat în acest sens. Accesul trebuie interzis pentru persoanele autorizate care își schimbă locul de muncă.

8.2.8. Detectarea Tentativelor de Acces Neautorizat

Procesele de înregistrare și verificare a activității sistemelor de operare, conturilor utilizator și programelor trebuie să fie funcționale pe toate sistemele active (host, server, echipamente de rețea).

Vor fi activate funcțiile de anunțare a persoanelor responsabile oferite de firewall-uri și sistemele de control al accesului la rețea.

Vor fi activate funcțiile de înregistrare a evenimentelor pe dispozitivele firewall și pe toate

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 10 din 18
		Exemplar nr.: 1

sistemele de control al accesului.

Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examine) zilnic de către responsabilul IT.

Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie și pentru dispozitivele de tip firewall sau dispozitive de control al accesului.

Înregistrările de verificare pentru serverele și host-urile din rețeaua internă trebuie revizuite cel puțin săptămânal. Se vor verifica periodic (săptămânal) programele utilitare pentru detectarea tentativelor de acces neautorizat.

Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.

Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către responsabilul IT.

Utilizatorii sunt obligați să raporteze orice anomalii în performanța sistemelor utilizate cât și orice semne ale unor posibile infrațiuni la responsabilul IT.

8.2.9. Modificări și Modernizări ale Sistemului Resurselor Informaticice și de Comunicații
Orice modificare asupra unei componente a Sistemului Resurselor Informaticice și de Comunicații din cadrul Primăriei Pausesti, cum ar fi: sisteme de operare, componente hardware, echipamente și componente de rețea, aplicații, trebuie să urmeze procedurile în vigoare.

Compartimentul IT trebuie să fie anunțat de toate modificările care afectează mediul de funcționare a sistemului .

Toate propunerile de modernizare și extindere a elementelor de infrastructură a sistemului vor fi documentate și aprobate de către conducătorul entității. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a sistemului. Modificările și modernizările sistemelor de calcul vor fi documentate de către utilizator și aprobate de către conducerea instituției.

8.2.10. Utilizare Internet și Intranet

Programele pentru acces la rețeaua Internet sunt destinate utilizatorilor autorizați pentru a fi folosite în scopuri exclusiv de servicii.

Toate programele utilizate pentru acces la rețeaua Internet trebuie să facă parte din pachetul de programe aprobat de către Compartimentul IT. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziție de către producător. Toate fișierele care provin din rețeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puțin o dată la 24 ore. Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy și/sau firewall.

Nu se vor publica pe sit-urile web ale Primăriei Pausesti materiale cu caracter ofensiv sau de hărțuire, materiale publicitare comerciale sau personale.

Nu este permisă utilizarea resurselor informatice și de comunicații ale entității în scop personal sau pentru solicitări personale.

Cumpărăturile pe internet care nu au legătură cu atribuțiile de serviciu sunt interzise. Cumpărăturile în interes de serviciu se vor supune regulilor de achiziție ale Primăriei Pausesti.

Orice material confidențial al Primăriei Pausesti transmis prin rețeaua Internet trebuie criptat.

Fișierele electronice se supun aceluiași reguli de păstrare ce se aplică și altor documente și trebuie păstrate în conformitate cu regulile stabilite prin prezentele reglementări și

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 11 din 18
		Exemplar nr.: 1

reglementari proprii fiecărui compartiment.

Este interzisă accesarea site-urilor cu caracter pornographic, folosirea programelor peer-to-peer (exemple: Yahoo messenger, MSN, DC++, etc.), descărcarea/instalarea programelor din rețeaua Internet

8.2.11. Administrarea Conturilor

Prin acord individual, fișa postului și/sau alte documente toți utilizatorii acceptă prevederile privind securitatea sistemului resurselor informatice și de comunicații.

Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces.

Conturile utilizator ale persoanelor plecate din Instituție pe timp îndelungat (mai mult de 90 de zile) vor fi dezactivate (conturile nu vor mai putea fi accesate). Toate conturile utilizator care nu au fost accesate timp de 30 de zile vor fi dezactivate. După încă 30 zile conturile vor fi șterse dacă nu s-a solicitat accesul la acestea.

Responsabilul IT este responsabil de ștergerea conturilor persoanelor (utilizatorilor) care nu mai lucrează în entitate sau care nu mai au relații cu entitatea.

8.2.12. Parole de Acces

Parolele de acces din cadrul entității trebuie să îndeplinească următoarele condiții:

- Să fie schimbate de utilizator în mod regulat, cel puțin o dată la 90 de zile;
- Să aibă o lungime minimă de 6 caractere;
- Să fie parole complexe;
- Reutilizarea parolelor este interzisă;
- Parolele stocate trebuie criptate;

Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaților care răspund de securitatea sistemelor informatice. Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.

Responsabilul IT nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ. Utilizatorii nu pot folosi programe de stocare a parolelor.

Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă.

Procedurile de schimbare a parolei asistate de responsabilul IT trebuie să respecte următoarea procedură:

« Utilizatorul se va legitima, administratorul va verifica drepturile de acces a persoanei la contul utilizator; Se va genera o parolă care va fi comunicată utilizatorului »

8.2.13. Sistemul de Mesagerie Electronică

În cadrul Primăriei Pausesti următoarele activități sunt interzise:

- Trimiterea de mesaje cu caracter de intimidare sau hărțuire;
- Folosirea sistemului de mesagerie electronică în scopuri personale;
- Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
- Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
- Folosirea altei identități decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.
- Folosirea programelor de poștă electronică neautorizate.

În cadrul Primăriei Pausesti următoarele activități sunt interzise deoarece împiedică buna funcționare a comunicațiilor în rețea și eficiența sistemelor de mesagerie electronică:

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I
		Nr.de ex.: 5
COMISIA	Cod: P.S. 12.02	Revizia: -
		Nr.de ex. :-
		Pagina 12 din 18
		Exemplar nr.: 1

- Trimiterea sau retrimiteră email-urilor în lanț;
- Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituția.
- Trimiterea mesajelor de dimensiuni foarte mari;
- Trimiterea sau retrimiteră mesajelor ce pot conține viruși.

Toate informațiile și datele confidențiale ale Primăriei, transmise către alte rețele externe, trebuie să fie criptate.

Utilizatorii nu trebuie să trimită, retrimite, primească sau să stocheze informații confidențiale sau nesigure, ce privesc entitatea, folosind dispozitive de comunicații mobile care nu sunt autorizate. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenți digitali personali, pagere ce permit trimiterea/primirea de informații și telefoanele mobile.

8.2.14. Detectarea virușilor

Toate stațiile de lucru de sine stătătoare sau conectate la rețeaua de comunicații a Primăriei Pausesti, trebuie să utilizeze programe antivirus aprobate de către Responsabilul IT.

Programele antivirus nu trebuie dezactivate. Configurația programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.

Frecvența actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

Orice server de fișiere conectat la rețeaua Instituției trebuie să utilizeze un program antivirus aprobat în scopul detectării și curățirii virușilor care pot infecta fișierele puse la dispoziție.

Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat și trebuie să respecte regulile de instalare și utilizare a acestui program.

Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate și trebuie raportat imediat Responsabilului IT și conducerii entității.

8.2.15. Licențe de utilizare

Instituția publică trebuie să furnizeze un număr suficient de copii cu Licență pentru toate programele aprobate spre utilizare astfel încât angajații să își poată desfășura munca într-un mod eficient și rapid.

De asemenea, trebuie să se pună de acord în mod adecvat cu furnizorii implicați pentru obținerea de copii adiționale ale licențelor dacă și când acestea sunt necesare în activitatea instituției. Copiile suplimentare ale materialelor protejate prin drepturi de autor nu vor fi stocate pe sistemele sau resursele rețelei Primăriei în situația în care nu există aprobări specifice.

Programele sau alte bunuri informatice aflate sub incidența drepturilor de autor aflate în posesia Primăriei Pausesti nu vor fi copiate, cu excepția cazului în care această copiere este în concordanță cu prevederile licenței.

8.2.16. Relații cu terți

Orice activitate desfășurată de furnizor care implică acces la resursele informatice și de comunicații trebuie să se conformeze reglementările în vigoare ale Primăriei Pausesti.

În toate convențiile și contractele încheiate cu Furnizori trebuie specificate următoarele:

- Informațiile din cadrul Primăriei, la care Furnizorul are drept de acces;
- Modul în care informațiile la care Furnizorul are drept de acces urmează a fi protejate de către acesta precum și măsuri ce vor fi luate în cazul nerespectării clauzelor;
- Metodele de predare, distrugere sau de transfer al drepturilor informațiilor Instituției aflate în posesia Furnizorului, la încheierea contractului.

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I
		Nr.de ex.: 5
COMISIA	Cod: P.S. 12.02	Revizia: -
		Nr.de ex. :-
		Pagina 13 din 18
		Exemplar nr.: 1

Furnizorul trebuie să folosească sistemul de resursele informatice si de comunicatii din cadrul Primariei numai în scopul stipulat în contract.

Orice altă informație din sistemul resurselor informatice si de comunicatii al Primariei obținută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.

Toate echipamentele de întreținere ale Furnizorului, aflate în rețeaua internă a Primariei și care se pot conecta în exterior prin intermediul rețelei, a liniilor telefonice sau a liniilor închiriate, precum și toate conturile de utilizator create temporar pentru Furnizor și necesare pentru acces la resursele informatice si de comunicatii vor fi scoase din uz la încheierea relațiilor contractuale.

Accesul Furnizorului trebuie să fie identificat în mod unic iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu reglementările interne menționate.

Activitățile principale ale Furnizorului trebuie să fie documentate de acesta și puse la dispoziția conducerii Instituției, la cerere. Acestea trebuie să cuprindă, dar să nu fie limitate la, evenimente precum: schimbări de personal, schimbări de parolă, schimbări majore în derularea proiectului, timpii de sosire, de plecare și de livrare.

În cazul retragerii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informațiile sensibile sunt colectate și predate Primariei sau distruse în cel mult 24 de ore de la producerea evenimentului.

În cazul terminării/rezilierii contractului sau la cererea Primariei, Furnizorul va preda sau distruge toate informațiile ce aparțin Instituției și va oferi certificare în scris privind predarea sau distrugerea informațiilor în decurs de 24 de ore de la producerea evenimentului.

În cazul încheierii contractului sau la cererea Primariei, Furnizorul trebuie să predea imediat toate legitimațiile, cartelele de acces, echipamentele și stocurile Primariei. Echipamentele și/sau stocurile care urmează a fi reținute de către Furnizor trebuiesc documentate și autorizate de conducerea Primariei.

Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către Instituția publică trebuie să fie inventariate corespunzător și să posede drepturi de utilizare atestate prin Licențe.

8.3. EXPLOATAREA RESURSELOR INFORMATICE SI DE COMUNICATII INSTRUCTIUNI DE LUCRU (I.L.)

8.3.1. Intervenții în cazul defecțiunilor hardware

În cazul în care a fost constatată o defecțiune sau o disfuncționalitate a vreunui sistem de calcul și/sau a unui periferic al acestuia (monitor, tastatură, mouse, imprimantă, etc) se va informa responsabilul IT din cadrul Compartimentului IT.

Poate exista și cazul în care defecțiunea să fie constatată de către responsabilul IT când acesta execută operațiuni de întreținere sau verificări de rutină.

Responsabilul IT va constata în ce constă defecțiunea și dacă este posibil va proceda la remedierea acesteia. În cazul în care nu este posibilă remediere de către specialistul IT, acesta va anunța firma de service, conform instrucțiunii de lucru.

Reprezentantul firmei de service va stabili dacă defecțiunea poate remedia pe loc, în cadrul instituției, sau este necesară deplasarea componentei hardware defecte la sediul firmei. După remedierea defecțiunii se va proceda la recepția componentelor hardware.

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 14 din 18
		Exemplar nr.: 1

8.3.2. Salvările de date, stocarea și păstrarea acestora

Salvările de date în general se fac pe suport magnetic extern (dischete, CD, benzi magnetice, memory stick), sau pe suport magnetic intern (hard disk) în funcție de instrucțiunile existente în manualele programelor informatice. De asemenea perioada de păstrare a acestor salvări se va face tot în funcție de aceste instrucțiuni. Dacă nu există instrucțiuni în acest sens păstrarea se va face pe perioadă nedeterminată.

În cazul salvărilor efectuate pe harddiskurile serverelor prin opțiunile existente în cadrul programelor informatice, se vor efectua salvări complete de către o persoană desemnată în acest sens de către șeful compartimentului respectiv.

Salvări complete ale harddiskurilor serverelor se va face de către responsabilul IT din cadrul Compartimentului IT.

Pentru salvările efectuate și pentru care nu există instrucțiuni privind termenul de păstrare a salvărilor, păstrarea se va face pe perioadă nedeterminată.

În cazul schimbării unui sistem informatic cu unul mai nou și în care au fost preluate datele existente în salvările efectuate anterior, vechile salvări vor fi distruse.

Persoanele care efectuează salvări vor avea un jurnal de evidență al acestor salvări în care se va specifica clar data și ora când a fost efectuată salvarea.

8.3.3. Achiziții echipamente hardware și/sau software pe bază de referat de necesitate, altele decât prin licitații

Pentru achiziționarea echipamente hardware și/sau software pe bază de referat de necesitate, referatul de necesitate înainte de a fi trimis spre aprobare conducerii instituției va fi avizat de către responsabilul IT pentru a stabili dacă necesitatea achiziționării echipamentelor este justificată sau nu. În cazul unui aviz favorabil referatul de necesitate va fi aprobat ulterior de către conducătorii instituției.

Referatele avizate și aprobate vor fi retransmise Compartimentului IT pentru a fi achiziționate echipamentele.

Dacă quantumul valorii echipamentelor depășește plafonul legal privind achiziția materialelor, acestea intrând pe lista de investiții, referatul respectiv va fi trimis de către Compartimentul IT compartimentului care se ocupă cu achizițiile publice .

8.3.4. Modificări sau defectiuni ale aplicațiilor software

În cazul în care sunt necesare modificări ale aplicațiilor software (programe informatice) în urma modificărilor legislative sau datorită altor cauze, sau constatării funcționării defectoase, sau a apariției unor erori de funcționare se va anunța în scris sau telefonic, sau prin email, sau prin fax, producătorul/autorul aplicației sau firma care ofera asistență, după caz.

Compartimentul care solicită modificările va furniza date cât mai amănunțite astfel încât modificările realizate să fie corecte.

Compartimentul care solicită modificarea este răspunzător de datele furnizate.

Realizatorul modificărilor este răspunzător de modificările aduse în aplicația software. Acesta este obligat să informeze sau să instruiască utilizatorii aplicațiilor despre modificările aduse.

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 15 din 18
		Exemplar nr.: 1

În cazul defecțiunilor dacă se va constata că erorile de funcționare se datorează unor defecțiuni ale echipamentului hardware se va anunța responsabilul IT și se va urma instrucțiunea de lucru privind ”Intervenții în cazul defecțiunilor hardware”.

8.3.5. Exploatarea aplicațiilor informatice

Exploatare/utilizarea aplicațiilor informatice se face doar de către personalul autorizat în conformitate cu instrucțiunile prevăzute în manualul aplicației.

Utilizatorii noi care vor utiliza un program informatic vor fi instruiți de către persoanele abilitate în acest sens, de exemplu utilizatori cu vechime în exploatare acestuia sau de către un reprezentant al producătorului.

În cazul unui program informatic nou instruirea se face de către un reprezentant al producătorului programului informatic.

Dacă apar modificări din diverse motive se va urma instrucțiunea „Modificări sau defecțiuni ale aplicațiilor software”.

8.3.6. Activități de mentenanță privind componentele hardware

Activități de mentenanță privind componentele hardware se vor executa cel puțin o dată pe lună la stațiile de lucru de către firma de service, iar pentru servere se va executa cel puțin o dată pe săptămână de către responsabilul IT din cadrul Compartimentului IT și o dată pe lună de către firma de service.

Verificările de rutină efectuate se vor evidenția într-un jurnal de activități.

În cazul constatării unor nereguli în funcționarea echipamentelor în urma acestor verificări se va urma instrucțiunea privind „intervențiile în cazul defecțiunilor hardware”.

8.3.7. Poșta electronică, sesizări pe site-ul primăriei, sesizări pe alte site-uri de specialitate

Mesajele sosite pe cale electronică: e-mailuri, sesizări postate pe site-ul primăriei sau sesizări postate pe alte site-uri de acest gen, vor fi listate pe suport de hârtie și depuse la registratura generală a instituției, după care vor fi direcționate către compartimentele de specialitate din cadrul instituției.

În cazul în care unele din aceste mesaje necesită răspuns, acesta va fi întocmit de către compartimentele de specialitate din cadrul instituției.

8.3.8. Rezolvarea documentelor/problemei repartizate spre rezolvare

Documente/probleme repartizate spre rezolvare Compartimentului IT vor fi soluționate în cel mai scurt timp de către responsabilul IT, cu respectarea procedurilor de lucru și a regulamentelor de securitate a informației. În cazul în care vreun document/problemă repartizate duce la încălcarea vreunei proceduri de lucru sau a unei reguli de securitate se va înștiința în scris conducerea instituției despre această situație.

Dacă documentele nu sunt de competența Compartimentului IT acestea vor fi returnate spre registratura instituției.

8.3.9. Anunțarea defecțiunilor hardware/software firmei de service, garanții și/sau asistență

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I Nr.de ex.: 5
		Revizia: - Nr.de ex. :-
COMISIA	Cod: P.S. 12.02	Pagina 16 din 18
		Exemplar nr.: 1

În cazul apariției unei defecțiuni care nu poate fi rezolvată de către responsabilul IT din cadrul Compartimentului IT, după cum este prevăzut și în instrucțiune, se va contacta firma de service, garanții sau asistență hardware/software, după caz.

Anunțarea se va face telefonic, prin email, fax de către responsabilul IT. Intervenția prestatorului de service se va face cu respectarea termenelor în cazul intervențiilor prevăzute în contractul de service.

8.3.10 Părăsirea temporara a calculatorului. Oprirea Calculatorului

În cazul în care utilizatorul părăsește temporar calculatorul este obligat să blocheze stația de lucru prin utilizarea opțiunii "Log Off", în cazul în care stația este utilizată de mai mulți utilizatori, sau prin utilizarea opțiunii "Lock Computer". De asemenea este obligatorie selectarea opțiunii "On resume, password protect" din cadrul secțiunii "Screen Saver". Este interzisă cu desăvârșire părăsirea stației de lucru fără a închide aplicațiile în care se lucrează.

8.3.10. Atribuirea/schimbarea/anularea utilizatorilor și a parolelor de acces

Procedurile de schimbare a parolei asistate de responsabilul IT trebuie să respecte următoarea procedură:

- Utilizatorul se va legitima, responsabilul IT va verifica drepturile de acces a persoanei la contul utilizator;
- Se va genera o parolă care va fi comunicată utilizatorului
- Se va întocmi/actualiza fișa utilizatorului de către responsabilul IT.

În cazul în care un utilizator părăsește definitiv sau temporar instituția responsabilul IT va recurge la ștergerea contului acestei persoane.

8.4. Reguli privind utilizarea resurselor informatice

Utilizarea sistemului RIC se face numai în interes de serviciu.

Utilizatorii trebuie să anunțe responsabilul IT sau conducerea entitatii în cazul în care se observă orice problemă/breșă în sistemul de securitate a resurselor informatice și de comunicații cât și orice posibilă întrebuintare greșită sau încălcare a regulamentelor în vigoare.

Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și de comunicații și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip în cadrul sistemului.

Utilizatorii nu trebuie să încerce să obțină acces la date sau programe pentru care nu au autorizație sau consimțământ explicit.

Utilizatorii nu trebuie să divulge nimănui numerele de acces Dialup sau Dialback prin modem.

Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive și/sau informații similare utilizate în scopuri de autorizare și identificare.

Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).

Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea responsabilului IT, cu excepția cazului în care acestea se găsesc pe lista programelor standard

COMUNA PAUSESTI	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I
		Nr.de ex.: 5
COMISIA	Cod: P.S. 12.02	Revizia: -
		Nr.de ex. :-
		Pagina 17 din 18
		Exemplar nr.: 1

folosite în cadrul Primăriei. Această listă va fi întocmită de către responsabilul IT împreună cu conducerea în funcție de necesitățile compartimentelor.

Utilizatorii nu trebuie:

- să se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane;
- să degradeze performanțele sistemului;
- să împiedice accesul unui utilizator autorizat la sistem;
- să obțină alte resurse în afara celor alocate;
- să nu ia în considerare măsurile de securitate impuse prin regulamente;
- să exploateze defectuos componentele sistemului;
- să utilizeze dischete, cd-uri, sau orice alt suport magnetic de stocare a informației din exteriorul instituției fără acordul explicit al responsabilului IT;

Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității sistemului. De exemplu, utilizatorii din primarie nu trebuie să ruleze programe de decriptare a parolilor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.

Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Primaria le poate considera ofensive, indecente sau obscene (altele decât cele pentru care aprobarea explicită a conducerii instituției).

Utilizatorii care au acces la sistem au obligația de a purta acte și/sau legitimații/ecusoane care să ateste calitatea de utilizator autorizat în spațiile Primăriei.

Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor Primăriei folosind resursele informatice și de comunicații.

În cazul demisiei/plecării definitive din instituție a unui utilizator acest lucru va fi comunicat responsabilului IT de către Serviciul Resurse Umane din Cadrul instituției. Responsabilul IT va recurge la stergerea conturilor și parolilor utilizatorului respectiv, iar accesul utilizatorului la sistem va fi interzis.

Este interzisă utilizarea sistemului de către persoane neautorizate.

9. Responsabilități și răspunderi în derularea activității

Primarul :

-Responsabil la nivelul Instituției publice cu administrarea și finanțarea resurselor informatice și de comunicații.

-Responsabil privind crearea, modificarea și aprobarea regulamentelor privind activitățile de finanțare, administrare și utilizare a resurselor informatice și de comunicații.

Responsabil cu Securitatea resurselor informatice și de comunicații (specialistul IT din cadrul instituției):

-Răspunde de administrarea funcțiilor de securitate a informației în cadrul Instituției publice.

-Este persoana de contact intern și extern a Instituției publice pentru orice problemă în legătură cu securitatea resurselor informatice și de comunicații.

Utilizatori:

-Persoane autorizate de către Instituția publică să folosească, în conformitate cu procedurile și regulamentele în vigoare, resursele informatice și de comunicații.

COMUNA PAUSESTI COMISIA	MANAGEMENTUL SISTEMULUI INFORMATIC	Ediția: I
		Nr.de ex.: 5
	Cod: P.S. 12.02	Revizia: -
		Nr.de ex. :-
		Pagina 18 din 18
		Exemplar nr.: 1

10. Anexe, inregistrari, arhivari

10.01. Anexe

Nr. Crt.	Denumire anexa	Elaborator	Aproba	Nr. ex.	Difuzare	Arhivare		Alte elem.
						Loc	Perioada	
1.	Coperta	-	-	-	-	Arhiva	Cf. N.A.	

10.2. Difuzare:

Procedura este pusa la dispozitia compartimentelor U.A.T.C. Pausesti in format de hartie sau in format electronic pe baza **Listei de difuzare-controlata**, formular cod **PS 00/F1**.

11. Cuprins

Numărul componentei în cadrul procedurii operaționale	Denumirea componentei din cadrul procedurii operaționale	Pagina
	Coperta	0
1.	Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii	1/18
2.	Situația edițiilor și a reviziilor în cadrul edițiilor procedurii	1/18
3.	Lista cuprinzând persoanele la care se difuzează ediția sau, după, caz, revizia din cadrul ediției procedurii	1/18
4.	Scopul procedurii	2/18
5.	Domeniul de aplicare a procedurii	2/18
6.	Documentele de referinta (reglementari) aplicabile activitatii procedurate	2/18
7.	Definitii si abrevieri ale termenilor utilizati in procedura	3/18
8.	Descrierea procedurii formalizate	5/18
9.	Responsabilitati si raspunderi in derularea activitatii	17/18
10.	Anexe, inregistrari, arhivari	18/18
11.	Cuprins	18/18

COMUNA PAUSESTI COMISIA	PROCEDURA DE SISTEM	Ediția: 1
	MANAGEMENTUL SISTEMULUI	Nr.de ex.: 1
	INFORMATIC	Revizia: -
	LISTA DE DIFUZARE	Nr.de ex. :-
	Cod: P.S. 00/F1	Pagina 1 din 1
		Exemplar nr.: 1

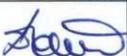
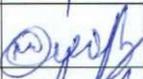
Lista cuprinzând persoanele la care se difuzează ediția sau, după caz, revizia din cadrul ediției procedurii de sistem:

Nr. crt.	Scopul difuzarii	Ex. nr.	Compartiment	Funcția	Nume si prenume	Data primirii	Semnatura
0	1	2	3	4	5	6	7
3.1	Aplicare	1	Financiar-contabilitate, achizitii publice, resurse umane-salarizare	Inspector	Bobilca Dan	29.12.2017	
			Registrul Agricol	Consilier	Chitoiu Ana Maria	29.12.2017	
			Asistență socială	Asistent comunitar	Mateescu Anghel Mircea	29.12.2017	
			Impozite si taxe	Inspector	Bizic Dumitru	29.12.2017	
			Casierie	Referent	Ilie Nicolae	29.12.2017	
			Cultura	Bibliotecar	Toabes Elena	29.12.2017	
			Juridic, Stare civila, registratura	Consilier	Popa Maria	29.12.2017	
				Consilier Juridic	Calin Florentina	29.12.2017	
			Serviciul situatii de urgenta	Consilier	Pitigoi Ion	29.12.2017	
			Administrativ	Guard	Cruceru Viorica	29.12.2017	
3.2	Informare	2	Cabinet primar	Consilier personal	Stanisor Mirabela	29.12.2017	
3.3	Evidenta	3	Comisie	Secretar comisie	Chitoiu Ana Maria	29.12.2017	
3.4	Control SCIM	4	Comisie	Presedinte	Paloiu Daniela	29.12.2017	
3.5	Arhivare	5	Arhiva	Responsabil arhiva	Toabes Elena	29.12.2017	

COMUNA PAUSESTI	PROCEDURA DE SISTEM REALIZAREA PROCEDURILOR FORMALIZATE PE ACTIVITATI	Ediția: 1
		Nr.de ex.: 1
COMISIA	<u>ANALIZA SI AVIZARE</u> <u>Cod: P.S. 00 F0</u>	Revizia: 0
		Nr.de ex. :-
		Pagina 1 din 1
		Exemplar nr.: 1

Cod procedura: **P.S. 12.02**

Denumire Procedura: **MANAGEMENTUL SISTEMULUI INFORMATIC**

Comisie/ compartiment	Nume si prenume	Functia	Aviz favorabil		Aviz nefavorabil		
			Semnatura	Data	Observatii	Semnatura	Data
Comisia de lucru in vederea monitorizării, coordonării și îndrumării metodologice cu privire la sistemul propriu de control managerial	Paloiu Daniela	Presedinte		27.12.2017			
	Bobilca Dan	Vicepresedinte		27.12.2017			
	Bizic Dumitru Marius	Membru		27.12.2017			
	Fota Mihai	Membru		27.12.2017			
	Popa Maria	Membru		27.12.2017			
	Mateescu Anghel Mircea	Membru		27.12.2017			
	Toabes Elena	Membru		27.12.2017			
	Pitigoi Ion	Membru		27.12.2017			
	Chitoiu Ana Maria	Secretar		27.12.2017			