

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 1 din 11

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

	Elemente privind responsabilii / operațiunea	Numele și prenumele	Funcția	Data	Semnătura
	1	2	3	4	5
1.1.	Elaborat	Șerban Codruț Valeriu	Referent		
1.2.	Verificat	Șerban Codruț Valeriu	Referent		
1.3.	Avizat	Rusu Cristina	PC		
1.4.	Aprobat	Hrițcu Gheorghe	Primar		

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 2 din 11

2. Formular evidență modificări

	Nr. ediției/ reviziei	Data ediției/ reviziei	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediției sau reviziei ediției	Avizul conducătorului compartimentului în cadrul căruia s-a elaborat procedura
	1	2	3	4	5	6
2.1.	Ediția I		X	X		
2.2.	Revizia 0					

3. Formular distribuire procedură

[illegible]

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 4 din 11

4. SCOP

4.1. Procedura este întocmită în scopul de a asigura condițiile și modul de funcționare a sistemului informatic și stabilirea regulilor, normelor și a măsurilor de siguranță și protecție a datelor și informațiilor din sistemul informatic integrat.

4.2. Dă asigurări cu privire la existența documentației adecvate derulării activității.

4.3. Asigură continuitatea activității, inclusiv în condiții de fluctuație a personalului.

4.4. Sprijină auditul și/sau alte organisme abilitate în acțiuni de auditare și/sau control, iar pe manager, în luarea deciziei.

5. DOMENIUL DE APLICARE

5.1 Procedura se aplică de către **Responsabilul Informatică**, la toate compartimentele și birourile ce deservește **primăria U.A.T.**, ce folosesc sistemul informatic în ceea ce privește aparatura IT și softurile ce deservește fiecare serviciu în parte.

6. DOCUMENTE DE REFERINȚĂ

6.1. Reglementări internaționale

6.1.1. Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

6.2. Legislație primară

6.2.1. Legea nr. 455/2001 privind semnătura electronică, republicată (r1).

6.2.2. Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, cu modificările și completările ulterioare.

6.2.3. Legea nr. 64/2004 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001

6.2.4. Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.

6.2.5. Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

6.2.6. Legea nr. 129/2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date

6.2.7. Ordonanța nr. 25/2006 privind întărirea capacității administrative a Oficiului Român pentru Drepturile de Autor, republicată (r1), cu modificările și completările ulterioare.

6.3. Legislație secundară

6.3.1. Hotărârea nr. 1007/2001 pentru aprobarea Strategiei Guvernului privind informatizarea administrației publice.

6.3.2. Ordinul nr. 600/2018 pentru aprobarea Codului controlului intern managerial al entităților publice, emis de Secretariatul General al Guvernului.

6.3.3. Ordinul nr. 252/2003 pentru aprobarea Normelor metodologice privind instruirea și specializarea în domeniul informaticii a funcționarilor publici

6.3.4. Ordinul nr. 461/2009 pentru aprobarea Strategiei naționale privind implementarea serviciului universal în sectorul comunicațiilor electronice.

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 5 din 11

6.3.5. Ordinul nr. 473/2009 privind procedura de acordare, suspendare și retragere a deciziei de acreditare a furnizorilor de servicii de certificare

6.3.6. Decizia nr. 99/2018 privind încetarea aplicabilității unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date

6.4. Alte documente, inclusiv reglementări interne ale entității publice

6.4.1. ROF, ROI, Planuri de acțiuni.

6.4.2. Dispoziția Primarului pentru numirea Comisiei de monitorizare, coordonare și îndrumare metodologică pentru dezvoltarea sistemului de control intern managerial.

6.4.3. Regulament de organizare și funcționare a Comisiei de monitorizare, coordonare și îndrumare metodologică pentru dezvoltarea sistemului de control intern managerial.

7. DEFINIȚII ȘI ABREVIERI

7.1. Definiții ale termenilor:

7.1.1. *Administrator de sistem* – persoana care proiectează, dezvoltă, implementează, întreține în funcțiune soluții IT ce include lucrul în rețea și accesul la Internet, pune cele mai convenabile soluții la dispoziția angajaților și a conducerii, în funcție de specificul activităților desfășurate și de rezultatele așteptate;

7.1.2. *Colecții organizate de date* - baza de date, reprezintă mulțimea datelor supuse prelucrărilor și/sau evidenței computerizate;

7.1.3. *Computer* – este un mijloc electronic de prelucrat date și informații, conform unei liste de instrucțiuni numite program;

7.1.4. *Ediție procedură* – forma actuală a procedurii; ediția unei proceduri se modifică atunci când deja au fost realizate 3 revizii ale respectivei proceduri sau atunci când modificările din structura procedurii depășesc 50% din conținutul reviziei anterioare.

7.1.5. *Hardware* – totalitatea sistemelor de calcul folosite pentru prelucrarea și/sau evident datelor.

7.1.6. *Iesiri* – rezultatele prelucrărilor efectuate asupra datelor.

7.1.7. *Instanță* - Organ de stat însărcinat cu soluționarea litigiilor dintre persoanele fizice sau dintre acestea și persoanele juridice.

7.1.8. *Intrări* – totalitatea datelor supuse prelucrărilor.

7.1.9. *Număr ediție* - număr de ordine acordat documentului la elaborare și/sau la o modificare de anvergură.

7.1.10. *Număr revizie* - număr de ordine acordat la modificarea parțială a documentului (a unei secțiuni/ pagini).

7.1.11. *Prelucrări* – totalitatea operațiilor efectuate asupra datelor pentru obținerea informațiilor care stau la baza deciziilor;

7.1.12. *Procedură documentată* – modul specific de realizare a unei activități sau a unui proces, editat pe suport de hârtie sau în format electronic; procedurile documentate pot fi proceduri de sistem și proceduri operaționale.

7.1.13. *Procedură operațională (procedură de lucru)* - procedură care descrie un proces sau o activitate care se desfășoară la nivelul unui sau mai multor compartimente dintr-o entitate, fără aplicabilitate la nivelul întregii entități publice.

7.1.14. *Programul antivirus* – este folosit în general pentru prevenirea și eliminarea virusilor de computer, viermilor și cailor troieni.

7.1.15. *Program informatic* – reprezentarea sau implementarea unui algoritm într-un cod sursă.

7.1.16. *Resurse umane* – personal tehnic, utilizatori.

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 6 din 11

7.1.17. Revizie procedură - acțiunea de modificare respectiv adăugare sau eliminare a unor informații, date, componente ale unei ediții a unei proceduri, modificări ce implică de regulă sub 50% din conținutul procedurii.

7.1.18. Rețea locală – rețea de calculatoare ce acoperă, în general o arie locală, restransă: un birou, o clădire, un grup de clădiri alăturate.

7.1.19. Server – este un program de aplicație care furnizează servicii altor aplicații;

7.1.20. Sisteme de comunicații – intranet, internet, telecomunicații etc.

7.1.21. Sistemul informatic - sistem care permite introducerea de date prin procedee manuale sau prin culegere automată de către sistem, stocarea acestora, prelucrarea lor și extragerea informației (rezultatelor) sub diverse forme;

7.1.22. Software – totalitatea programelor folosite pentru prelucrarea și/sau evident datelor;

7.1.23. Strategia de securitate – este compusă din totalitatea normelor, regulilor, procedurilor, îndrumărilor de bună practică care protejează bunurile organizației: echipamente hardware de orice fel, produse, aplicații, component software de orice fel, date și orice alt fel de informații.

7.2. Abrevieri ale termenilor:

7.2.1. HG	= Hotărârea Guvernului
7.2.2. O.U.G.	= Ordonanța de Urgență a Guvernului României
7.2.3. SCIM	= Sistem de control intern/managerial
7.2.4. Comisie	= Comisia de monitorizare
7.2.5. P.O.	= Procedură operațională.
7.2.6. PC	= Președintele Comisiei
7.2.7. CI	= Coordonator de implementare
7.2.8. A.P.L.	= Administrație Publică Locală
7.2.9. R.O.F.	= Regulament de Organizare și Funcționare
7.2.10. R.O.I.	= Regulament de Ordine Interioară
7.2.11. SI	= Sistem informatic
7.2.12. BD	= Baza de date
7.2.13. ADMIN	= Administrator de sistem
7.2.14. IT	= Tehnologia informației
7.2.15. RIC	= Resurse Informatică și de Comunicație

8. DESCRIEREA ACTIVITĂȚII SAU PROCESULUI

8.1 Generalități

8.1.1. Resursele Informatică și de Comunicații puse la dispoziție și administrate de către **Responsabilul Informatică** sunt bunuri strategice ale **Primăriei** care trebuie administrate ca resurse ale statului român.

8.1.2. Compromiterea securității acestor resurse poate afecta capacitatea **Primăriei** de a oferi servicii informatice și de comunicații, poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilității instituției în fața partenerilor săi.

8.2 Politica de securitate

8.2.1. Politica de securitate este alcătuită astfel încât să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice publice, să stabilească practici prudente și acceptabile privind utilizarea Resurselor Informatică și de Comunicații ale Primăriei și să instruiască utilizatorii care au dreptul de folosire a Resurselor Informatică și de Comunicații privind responsabilitățile asociate unei astfel de utilizări.

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 7 din 11

8.2.2. Politica de securitate a Resurselor Informatice și de Comunicații ale Primăriei se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice RIC a instituției. Nu există niciun fel de conotații: politice, religioase, rasiale legate de prevederile politicii de securitate.

8.2.3. Scopul urmărit de politica de securitate este acela de asigurare a integrității, confidențialității și disponibilității informației, precum și stabilirea cadrului necesar pentru elaborarea regulilor și procedurilor de securitate.

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

8.2.5. *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 Primăriei sunt proprietatea instituției în condițiile legilor în vigoare. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la Resursele Informatice și de Comunicații.

8.2.6. *Disponibilitatea* se asigură prin funcționarea continuă a tuturor componentelor Resurselor Informatice și de Comunicații.

8.3. Clasificarea informațiilor

8.3.1. Clasificarea informațiilor este necesară pentru a permite atât alocarea resurselor necesare: protejării 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 și strict secrete.

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

Exemple: Informațiile de pe avizare, servere web publice, știrile de presă.

8.3.3. Secrete: În această categorie se includ informațiile care datorită valorii economice nu trebuie făcute publice. Se includ aici și informațiile pe care Primăria trebuie să le protejeze conform legislației în vigoare. Datorită valorii economice asociate, aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate și distribuite în cadrul Primăriei doar utilizatorilor autorizați. Distribuirea acestor informații de către utilizatorii autorizați trebuie să se facă pe baza unei clauze de confidențialitate.

Exemple, clauze contractuale, conturi și parole folosite pe serverele de contabilitate sau gestiune.

8.3.4. Strict secrete sau confidențiale: În această categorie se includ toate informațiile care datorită valorii economice nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidența Codului Civil, Penal sau legislației fiscale. Accesul la aceste informații va fi restricționat. Datele strict secrete nu pot fi copiate, distribuite sau șterse fără acordul scris al conducerii Primăriei.

Exemple: cheile criptografice, conturi administrative de pe serverele de contabilitate.

8.4. Planul de securitate al rețelelor IT

8.4.1. Planul de securitate are ca scop principal protejarea utilizatorilor și colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea, acesta are ca scop protejarea imaginii Primăriei și a investițiilor acesteia pentru dezvoltarea sistemului informatic și de comunicații, protejarea proprietății intelectuale și a tuturor informațiilor stocate și transportate cu ajutorul Resurselor Informatice și de Comunicații ale utilizatorilor autorizați: funcționari publici, personal contractual, colaboratori etc.

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 8 din 11

8.4.2. Utilizarea Resurselor Informatice și de Comunicații se face numai în interes de serviciu.

8.4.3. Utilizatorii trebuie să anunțe **Responsabilul Informatică**, atât despre orice problemă/breșă în sistemul de securitate din cadrul Primăriei, cât și despre orice posibilă întrebuintare greșită sau încălcare a regulamentelor în vigoare.

8.4.4. Prin acțiunile lor, utilizatorii 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 Resurselor Informatice și de Comunicații ale Primăriei.

8.4.5. Utilizatorii nu trebuie să încerce să obțină acces la date sau programe din Resursele Informatice și de Comunicații pentru care nu au autorizație sau consimțământ explicit.

8.4.6. Utilizatorii nu trebuie să divulge sau să înstrăineze nume de conturi, parole, sau orice dispozitive și/sau informații similare utilizate în scopuri de autorizare și identificare.

8.4.7. Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală și a dreptului de autor (copyright).

8.4.8. Utilizatorii nu trebuie:

- a) să se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane;
- b) să degradeze performanțele sistemelor ce alcătuiesc Resursele Informatice și de Comunicații;
- c) să împiedice accesul unui utilizator autorizat la Resursele Informatice și de Comunicații;
- d) să obțină alte resurse în afara celor alocate;
- e) să nu ia în considerare măsurile de securitate impuse prin regulament.

8.4.9. Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității sistemelor ce alcătuiesc Resursele Informatice și de Comunicații.

8.4.10. Resursele Informatice și de Comunicații ale Primăriei nu trebuie să fie folosite pentru beneficiul personal.

8.4.11. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Primăria le poate considera ofensive, indecente sau obscene.

8.4.12. Angajații nu trebuie să permită membrilor familiei sau altor persoane accesul la Resursele Informatice și de Comunicații ale Primăriei.

8.4.13. Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor Primăriei folosind Resursele Informatice și de Comunicații.

8.4.14. Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Primăriei sau prejudicierea, indiferent de formă, a intereselor Primăriei.

8.4.15. Toate mesajele, fișierele și documentele localizate în cadrul Resurselor Informatice și de Comunicații sunt proprietatea Primăriei și pot fi subiectul unor cereri de verificare/inspectare/accesare.

8.5. Reguli de securizare a serverelor

8.5.1. Procedura de securizare a serverelor trebuie să includă, obligatoriu, următoarele:

1. Instalarea sistemului de operare dintr-o sursă aprobată;
2. Înlăturarea programelor, a serviciilor sistem și a driver-elor care nu sunt necesare;
3. Setarea/activarea parametrilor de securitate, a protecțiilor pentru fișiere;
4. Dezactivarea sau schimbarea parolelor conturilor predefinite;
5. Securizarea accesului fizic la aceste echipamente.

8.6. Reguli privind parolele de acces

Orice parolă ar trebui să fie complexă și să aibă o lungime minimă de 8 caractere. O parolă complexă este un șir de caractere compus din litere minuscule, majuscule, cifre și simboluri (%\$#&^* ...).

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 9 din 11

Criterii pentru stabilirea unei parole:

- nu este deloc recomandată folosirea simplă a datelor personale (ex: data nașterii, nume, prenume etc.) ca parole;
- folosiți cifre și simboluri ușor de asociat prin forma lor cu litere. De exemplu: a = @, B=8, E=3, i=1, I=!, O=0(zero), s=\$.

Nu se vor nota parolele pe hârtii.

Nu se va folosi aceeași parolă pentru mai multe conturi.

Dacă aveți multe parole le puteți scrie într-un fișier, însă criptați acel fișier și asigurați-vă că nu-l veți pierde. Evitați denumirea celui fișier cu una explicită (parolelele.rar).

Evitați să păstrați parole în agende electronice, telefoane mobile - pot fi furate.

Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puțin o dată la 90 de zile.

Se va avea grijă la facilitatea browser-elor de reținere a parolelor (AutoFill, Remember password) cu atât mai mult atunci când calculatorul e folosit de mai multe persoane.

Parolele de cont utilizator nu trebuie divulgate nimănui.

Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.

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

Schimbarea parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:

- utilizatorul se va legitima;
- administratorul va verifica drepturile de acces ale persoanei la contul utilizator;
- utilizatorul va introduce o nouă parolă.

8.7. Reguli de administrare a conturilor de email

Fiecare cont de email creat pentru Primărie trebuie să aibă asociate o cerere și o aprobare corespunzătoare.

Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces. Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.

Toate parolele pentru conturi trebuie să fie create și folosite în conformitate cu Regulile privind Parolele de Acces.

Utilizatorilor nu le este permis să păstreze în directoarele proprii de pe server (Inbox, Sent, Trash) mesaje mai vechi de 6 luni. Excepție de la această regulă fac persoanele care au funcții de conducere, precum și cele din secretariat.

Pentru păstrarea tuturor mesajelor primite este necesară instalarea unui client local de email (ex: Outlook express etc.) pe calculatorul individual al fiecărui utilizator.

La cererea conducerii Primăriei, **Responsabilul Informatică** trebuie să furnizeze o listă cu toți utilizatorii (lista de conturi) pentru sistemele pe care le administrează.

8.8. Reguli privind sistemul de mesagerie electronică

8.8.1. Activități strict 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.

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 10 din 11

8.8.2. Activități interzise deoarece împiedică buna funcționare a comunicațiilor în rețea și eficiența sistemelor de mesagerie electronică:

- 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;

- Ignorarea cererii administratorului rețelei de a elibera spațiile de pe server pe care le ocupă.

Conform Regulilor de administrare a conturilor de email, toți utilizatorii (cu excepția persoanelor care au funcții de conducere și a celor din secretariat) se obliga să mențină în directoarele proprii de pe serverul de mail numai mesajele din cel mult ultimele 6 luni de zile.

8.8.3. Alte mențiuni privind securitatea informațiilor

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

- Toate activitățile utilizatorilor ce implică accesul și/sau folosirea resurselor informatice și de comunicații ale Primăriei pot fi oricând înregistrate și analizate.

- Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informații confidențiale sau nesigure, ce privesc Primăria, folosind dispozitive de comunicații mobile care nu sunt autorizate de Primărie. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: telefoane mobile, asistenți digitali personali, tablete ce permit trimiterea/primirea de informații.

8.9. Reguli privind detectarea virușilor

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

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 curățării 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 de 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 Informatică**.

8.10. Resurse necesare

8.10.1. Resurse materiale

Logistică: mobilier, rechizite, calculatoare, scanere, servere, software cu licență, rețea, imprimante, posibilități de stocare a informațiilor.

8.10.2. Resurse umane

Personalul din cadrul primăriei cu sarcini de serviciu stabilite în acest sens.

8.10.3. Resurse financiare

Cotă parte din cheltuielile generale ale primăriei în vederea achiziționării materialelor consumabile necesare acestei activități și asigurării serviciilor de întreținere a logisticii.

COMUNA SCOBINȚI PRIMĂRIE INFORMATICĂ	UTILIZAREA ȘI SECURITATEA REȚELELOR INFORMATICE ȘI DE COMUNICAȚII Cod: PO – INF – 02	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 11 din 11

9. RESPONSABILITĂȚI

Nr. crt.	Compartimentul (postul) / acțiunea (operațiunea)	I	II	III	IV	V	VI
	0	1	2	3	4	5	6
1	Responsabil Informatică -elaborează procedura -supraveghează la respectarea prevederilor prezentei proceduri -raspunde de alocarea și gestionarea parolelor de acces -pune în aplicare și rerespectă prevederile prezentei proceduri. -supraveghează funcționarea corectă a rețelelor informatice și de comunicații	E Ap					
2	Președintele Comisiei de monitorizare -Avizează prezenta procedură		Av				
3	Primarul -Asigură cadrul legislativ și organizatoric pentru desfășurarea activităților descrise în prezenta procedură; -Aprobă/reaprobă prezenta procedură			A			
Notă: E - elaborat V – verificat A – aprobat Ap - aplicat							

10. ANEXE, ÎNREGISTRĂRI, ARHIVĂRI

Nr. anexă	Denumirea anexei	Elaborator	Aprobă	Număr de exemplare	Difuzare	Arhivare		Alte elemente
						Loc	Perioada	
1								
2								

11. CUPRINS

Numărul componentei în cadrul procedurii operaționale	Denumirea componentei din cadrul procedurii operaționale	Pagina
	Coperta	
1	Lista responsabililor cu elaborearea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii operaționale.	1
2	Situația edițiilor și a reviziilor în cadrul edițiilor procedurii operaționale	2
3	Lista cuprinzând persoanele la care se difuzează ediția sau, după caz, revizia din cadrul ediției procedurii operaționale.	3
4	Scopul procedurii operaționale	4
5	Domeniul de aplicare a procedurii operaționale	4
6	Documentele de referință (reglementări) aplicabile activității procedurate	4
7	Definiții și abrevieri ale termenilor utilizați în procedura operațională	5
8	Descrierea procedurii operaționale	6
9	Responsabilități și răspunderi în derularea activității	11
10	Anexe, înregistrări, arhivări	11
11	Cuprins	11