Aprobat:
Primar,
Ing. Pavăl Vasile

Data: 13.10.2023

PROCEDURA OPERAȚIONALĂ
Tehnologia Informației
Cod: PO37-05-21
ed. 2, rev. 2

	Nume și prenume	Funcția	Data	Semnătura
Avizat	LĂCĂTUȘU EDUARD	Președinte Comisie Monitorizare	13.10.2023	
Verificat	BĂLȚATU RADU IONEL	Consilier superior	06.10.2023	
	HRISCU LILIANA	Secretariat Tehnic Comisie Monitorizare	06.10.2023	
Elaborat	FILARET BIANCA	Consilier superior	05.10.2023	

FORMULAR DE EVIDENȚĂ A MODIFICĂRILOR

Nr. cr.	Ediția/ Revizia	Data Ediției/Reviziei	Pag. modificata	Descrierea modificării	Semnătura conducătorului entitate organizatorică
1	2/0	17.12.2018		Implementarea cerintelor conform SR EN ISO 9001 :2015	
2	2/1	08.10.2020	Pag.8	modificare legislatie primara	
3	2/2	13.10.2023	Pag.6	modificare documente de referință	
4	2/2	13.10.2023	Pag.8	modificare legislatie primara, modificare legislatie primara	

FORMULAR DE ANALIZĂ PROCEDURĂ

Nr. crt.	Compartiment	Conducător compartiment Nume și prenume	Înlocuitor de drept sau delegat	Aviz favorabil		Aviz nefavorabil	Semnătura	Data
				Semnătura	Data	Observații		
1.	Direcția Economică	Boț Eugen			13.10.2023			
2.	Direcția de Gospodărie Urbană	Bălănescu Dorin			13.10.2023			
3.	Direcția de Amenajare a Teritoriului și Urbanism	Maftei Ana Alexandrina			13.10 2023			
4.	Directia Investitii, management Proiecte si supraveghere video	Frențescu Corina			13.10 2023			
5.	Serviciul Resurse Umane Organizare Securitate și Sănătate în Muncă	Șălaru Mariana			13.10 2023			

6.	Birou Achiziții Publice	Vasilescu Petronela			13.10.23			
7.	Serviciul Administrație Publică Locală	Prelipcean Iustin	Ionica Macan		13.10.2023			

LISTĂ DE DIFUZARE PROCEDURĂ

Nr. ex.	Compartiment	Nume şi prenume	Data primirii	Semnătura	Data retragerii	Data intrării în vigoare a procedurii	Semnătura
1	Birou Tehnologia Informației	Balțatu Radu Ionel	13.10.2023				
2	Birou Tehnologia Informației	Filaret Bianca	13.10.2023				
3	Birou Tehnologia Informației	Strătilă Alin Corneliu	13.10.2023				
4	Managementul Calitatii	Hriscu Liliana	13.10.2023				

CUPRINS

1. SCOP

Prin această procedura, Primaria Municipiului Vaslui :

Stabilește modul de realizare a activității, compartimentele și persoanele implicate.

Asigura continuitatea activităților, incluzând planul de acțiune în caz de dezastru.

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

Creeaza și menține o infrastructură de management informațional care presupune o interacțiune între oameni (utilizatori și Speclaliști IT), tehnologie (hardware, software și rețele) și procese (modul în care oamenii și sistemele interactioneaza). Aceasta interacțiune presupune monitorizare zilnica și ajustare permanenta pentru a crea sinergia și eficienta maxima. Pentru a sustine administrarea acestei activități complexe, procedurile sunt stabilite în cadrul Planului de securitate informatica și a Planului de Recuperare în caz de dezastru.

Acest document descrie urmatoarele elemente necesare administrării informației în cadrul PMV

- infrastructura IT și organizarea acesteia în cadrul PMV;
- planul de securitate informatică, care se referă la resursele, aplicațiile și alte date ca parte integrantă a administrarii infrastructurii informatlonale și securizarea organizației în viitor.
  Securizarea unui sistem presupune implementarea unui set de proceduri, reguli și tehnologii pentru a proteja infrastructura IT cat și a datelor din cadrul organizației. Atunci când calculatoarele se defectează, ori este intreruptă alimentarea cu energie, sau se întâmplă anumite dezastre, trebuie pus în aplicare un set de proceduri și procese.
- modalitatea de recuperare în cazul aparitiei unui dezastru care poate distruge infrastructura de comunicații.

2. DOMENIU de APLICARE

Procedura se aplica în cadrul PMV, și în zona de competență a Consiliului Local Vaslui.

3. DOCUMENTE de REFERINȚĂ

3.1. Reglementări internaţionale

- Legea 64/2004 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică;

3.2 Legislație primara

- Regulamentul (UE) 679/2016 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)
- Legea 455/2001 -privind semnatura electronică, cu modificările și completărilemulterioare.
- Legea 161/2003 -privind unele masuri pentru asigurarea transparenței în exercitarea demnitaților publice, a funcțiilor publice.
- OG nr. 25/2006 privind intărirea capacitții administrative a Oficiului Roman pentru Drepturile de Autori, republicată , cu modificarile și completarile ulterioare.
- Ordin 252/2003 (IT) - privind instuirea și specializarea în domeniul informaticii a funcționarilor publici, cu modificările și completărilemulterioare.
- HG 1259/2001 (IT) - privind aprobarea Normelor tehnice șsi metodologice pentru aplicarea Legii 455/2001 privind semnătura electronică, cu modificările și completărilemulterioare.
- Ordin 1155/2016 (IT) - privind emiterea prin intermediul centrului de imprimare masivă a unor acte administrative fiscale și procedurale.
- Legea 9/2023 - privind stabilirea unor măsuri de simplificare la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative.

3.3 Standarde de referință ale calității

SR EN ISO 9001:2015	Sisteme de management al calității. Cerințe
SR EN ISO 9000:2015	Sisteme de management al calității. Principii fundamentale și Vocabular
SR ISO / TR 10013: 2003	Linii directoare pentru documentația sistemului de management al Calității

3.4 Legislație secundară

- Legea 109/2007 - privind reutilizarea informațiilor din instituțiile publice, cu modificările și completărilemulterioare.
- Legea 8/1993 - privind dreptul de autor și drepturile conexe, cu modificările și completărilemulterioare.
- Ordinul secretarului general al Guvernului nr. 600/2018 pentru aprobarea Codului controlului intern/managerial al entităților publice;

3.5 Standarde de referință anti-mită

- ISO 37001:2016 - Sisteme de management anti-mită. Cerințe cu ghid de utilizare.

3.6 Reglementari interne

- Regulamentul de Organizare și Funcționare al Primariei Municipiului Vaslui ;
- Regulamentul de Ordine Interioară;

4. DEFINIŢII şi ABREVIERI

4.1. Definiții din standarde

Sunt utilizate definițiile din documentele de referință, și în plus urmatoarele:

1. **Sistemul informatic** = prelucarea automată a datelor din sistem (intrările) conform unor algoritmi prestabiliți, determinate de regulile de gestiune proprii fiecarei instituții și în conformitate cu reglementările și legislatia în vigoare.
2. **Intrări** = totalitatea datelor supuse prelucrărilor.
3. **Prelucrări** = totalitatea operațiilorlor effectuate asupra datelor pentru obtinerea informațiilor care stau la baza deciziilor.
4. **Hardware** = totalitatea sistemelor de calcul folosite pentru prelucarea și/sau evidența datelor.
5. **Software** = totalitatea programelor folosite pentru prelucrarea și/sau evidența datelor.
6. **Program informatic** = reprezentarea sau implementarea unui algoritm intr-un cod sursă.
7. **Server** = este un program de aplicație care furnizează servicii altor aplicații.
8. **Program antivirus** = este folosit în general pentru prevenirea și eliminarea virușilor de computer, viermilor și a cailor troieni.
9. **Expertii cu atributii IT** =
10. **Rețea informatică** = ansamblu de calcularoare interconectate prin intermediul unor medii de comunicații (cabluri metalice - coaxial, torsada, etcș fibră optivcă - mononod, multinodș linie telefonicaș ghid de undeș unde radio), în scopul utilizarii în comun, de către un număa mare de utilizatori, a tuturor resurselor informatice asociate calculatoarelor din rețea.
11. **Resurse informatice** (dintr-un sistem informatic) = resurse fizice ?(hardware), logice (software de bază și aplicații) și informaționale (baze de date și date proprii ale utilizatorilor autorizați) asociate calculatoarelor dintr-o rețea, împreună cu totalitatea mediilor de comunicație și a echipamentelor active care controlează comunicațiile în rețeaș la acestea se adaugă utilizatorii autorizați ai respectivului sistem imformatic, prin cunoștințele - specifice domeniului tehnologiei informațiilor și comunicațiilor - pe care aceștia le dețin și le utilizează in timp ce folosesc sistemul informatic respectiv.
12. **Configurație** = element descriptiv de bază cu privire la capacitatea funcțională și performanțele resurselor informatice.
11. **Strategia de securitate** : se compune din totalitatea normelor, regulilor, procedurilor, indrumarelor de bună practică care protejează bunurile organizației: echipamente hardware de orice fel, produse, aplicații, componente software de orice fel, date și orice altfel de informații.

4.2. Abrevieri

Sunt utilizate abrevierile din "Lista abrevierilor utilizate în documentele sistemului de management al calității din cadrul Primăriei Municipiului Vaslui " (anexă la Manualul Calității), și în plus urmatoarele:

- PMV = Primaria Municipiului Vaslui

- BIT = salariații din cadrul Biroului Tehnologia Informației
- ROF = Regulament de Orfine Interioara
- RL = rețea locala
- BD = baza de date
- IT = tehnologia informației
- SI = sistem informatic

5. DESCRIEREA ACTIVITĂȚILOR

5.1. Generalități

În vederea desfășurării activităților stabilite prin ROF, PMV depinde de infrastructura computerizată. În continuare este prezentată o descriere a organizării informației și a infrastructurii tehnice.

1. Îmbunătățirea preciziei rezultatelor prelucrărilor, prin eliminarea erorilor umane care pot apărea intr-un sistem manual de prelucare și de procesare uniformă a datelor, pe masura apariției lor;

2. Creșterea vitezei de procesare, prin prelucarea automată a datelor și eliminarea timpilor de prelucare manuală a acestora, oferind utilizatorilor informații solicitate, în momentul când aceștia au nevoie de ele;

3. Sporirea volumului de informații oferite utilizatorilor intr-un interval dat de timp, prin creșterea volumului de date prelucrate pe unitate de timp determinată de prelucrarea automată a acestora;

4. Salvarea datelor pe alte unități de stocare decat cele folosite în mod curent de către aplicații în vederea posibilității apariției unor defecte hardware, erori software, virusarea programelor, situații care pot determina pierderea datelor;

5. Controalele organizatorice sunt metode și tehnici de organizare a activităților desfasurate de institutie, folosite pentru prevenirea pierderilor și/sau alterărilor de date determinate de fraudă, neatentie și /sau neglijență, în vederea asigurării unui control intern eficient în sistemul de prelucrare a datelor utilizate de acestea;

În asigurarea controlului oricarui tip de sistem de prelucrare și evidență a datelor este definirea clară a funcțiilor, urmată de definirea și separarea locală a sarcinilor și responsabilităților angajaților pentru fiecare funcție, nici un angajat nu trebuie sa aibă sarcina și raspunderea completă pentru efectuarea unei activități; operația executată de o persoană trebuie verificată de o altă persoană.

6. Pentru asigurarea bunei funcționari a sistemului informatic, salariații din cadrul Biroului Tehnologia Informației au dreptul de a bloca accesul pe stațiile de lucru al persoanelor ce nu dețin anumite drepturi.

7. Utilizatorii își desfasoară activitatea prin programele puse la dispoziție de salariații Biroului Tehnologia Informației, utilizand user și parolă, acest lucru evidențiindu-se în rețea, iar accesul la internet a fiecarei stații de lucru este monitorizat în rețeaua de calculatoare prin alocarea unei adrese IP.

5.2.Obiectivele realizate prin buna funcționare a sistemului informatic

1. Asigurarea bunei funcționari și a reparațiilor componentelor sau calculatoarelor din dotatea instituției in masura competentelor in cazul in care nu se află în garanție la firmele producatoare;
2. Asigurarea asistenței tehnice de specialitate pentru achizițiile de echipamente IT noi, care să corespundă cerințelor echipamentelor existente și achiziției de calculatoare noi, conforme cu cerințele specifice ale PMV și la nivelul de performantă din momentul achiziției;
3. Asigurarea verificărilor periodice și intretinerea în stare de funcționare, in masura competentelor, a tuturor echipamentelor din dotarea PMV;
4. Asigurarea asistenței de specialitate, în măsura competențelor operatorilor IT cu privire la produsele software existente și executate de firme sau persoane autorizate care nu lucrează în instituție sau, în caz contrar, raportează erorile constatate;
5. Asigurarea asistenței utilizatorilor în utilizarea diferitelor tipuri de software;
6. Asigurarea asistenței în implementarea noilor produse software și asigurarea legăturii cu firmele producatoare sau cu persoanele de contact de la aceste firme;
7. Analizarea, proiectarea și dezvoltarea de aplicații personalizate diferitelor procese desfasurate în activitățile specifice în administratia publică;
8. Monitorizarea software-ului specific serverelor de baze de date;
9. Gestionarea conturilor de utilizator pentru accesarea aplicațiilor financiar-contabile pentru funcționarii din PMV;
10. Asigurarea funcționarii, dezvoltării , depanării rețelei de calculatoare existente și a tuturor echipamentelor specifice.

5.3. Descrierea activității

5.3.1. Organizarea activității

1. Instalarea soft-urilor achiziționate și intreținerea corespunzătoare a calculatoarelor, în acord cu contractele de licențiere încheiate;
2. Colaborarea cu utilizatorii cu privire la intreținerea soft-urilor specifice, asigurând configurarile hard și soft necesare instalării și funcționării acestora;
3. Asigurarea securității rețelei administrate, prevenirea și rezolvarea situațiilor de virusare a calculatoarelor din rețea;
4. Întreținerea și administrarea rețelei din interiorul PMV și a echipamentelor de conectare;
5. Localizarea și intervenția cu promptitudine în situația apariției unei defecțiuni în rețea, izolarea, remedierea problemei, in masura competentelor, și repunerea rețelei în situația de functionalitate, la parametrii permisi de defecțiunea respectivă;
6. Urmarirea depanării și recuperării echipamentelor hardware defecte;
7. Instalarea de dispozitive periferice specific, in masura competentelor, în colaborare cu furnizorii, ca: scanere, imprimante, multifuncționale, etc.
8. Asigurarea integrării de echipamente noi prin calcularea și realizarea extinderii rețelei existente;

9. Asigurarea coordonării și realizării activităților de intreținere a echipamentelor din componența rețelei, in masura competentelor;
10. Elaborarea de specificații tehnice necesare întocmirii caietelor de sarcini pentru achizițiile de tehnică de calcul și cablare în rețea;
11. Asigurarea compatibilitații sistemelor informatice specifice compartimentelor de specialitate cu problemele din softuri existente;
12. Asigurarea posibilității postării pe site-ul PMV a informațiilor specifice de interes public;
13. Asigurarea consilierii utilizatorilor cu privire la modul de utilizare a soft-ului destinat aplicațiilor locale, cat și a celui dedicat serviciilor Internet;
14. Asigurarea participării operatorilor la intreținerea și actualizarea bazelor de date și a serviciilor oferite: pagini intranet, scheme de subrețea, modificari ale tipologiilor rețelelor;
15. Asigurarea confidențialității documentelor și datelor folosite pentru rezolvarea unor probleme speciale sau pentru cercetare-documentare, în vederea realizarii unor aplicații noi.

5.3.2 Obiectivele compartimentului IT

1. Asigurarea depanării calculatoarelor, în măsura competențelor, la calculatoarele care nu se afla în termen de garanție cu recuperarea echipamentelor, în scopul reducerii cheltuielilor de exploatare și intreținere;
2. Asigurarea asistenței tehnice de specialitate pentru achizițiile de echipamente IT noi;
3. Verificarea calitații și stării tehnice a echipamentelor IT cumpărate în cadrul licitațiilor;
4. Asigurarea verificărilor periodice și intretinerea în stare de funcționare a tuturor calculatoarelor și a echipamentelor din PMV;
5. Asigurarea asistenței, în măsura competențelor, în ceea ce privește produsele software existente și executate de alte firme sau persoane autorizate din afara instituției; în caz contrar, contactează personalul de conducere și raportează erorile existente;
6. Asigurarea asistenței utilizatorilor în folosirea diferitelor produse software pentru a corespunde cerințelor proiectate;
7. Intretinerea și repararea softului specific serverelor de comunicații și de baze de date in masura competentelor;
8. Gestionarea conturilor de utilizator pentru accesarea internetului și a conturilor de e-mail pentru toti funcționarii din cadrul PMV.
9. Asigurarea funcționării , dezvoltării și depanării rețelei de calculatoare și a tuturor echipamentelor specifice;
10. Intocmirea Notei de fundamentare privind realizarea Planului anual de investitii pentru echipamente de calcul și extinderea rețelelor, necesare aducerii la parametrii optimi, în funcție de modificarile organizatorice și de personal din cadrul primariei.

5.3.3. Securitatea și confidențialitatea informațiilor

Toti angajații PMV au obligatia de a proteja confidențialitatea informațiior pe care le-au întalnit în timpul desfașurării atribuțiunilor de serviciu sau în orice alt mod.

5.3.4. Resurse necesare

5.3.4.1. Resurse materiale

5.3.4.1.1. Hardware și rețele

Calculatoarele din cadrul PMV sunt conectate intr-o rețea locală. Sistemele operationale sunt pe platforma Windows. Exista diferite servere în cadrul PMV, ele fiind situate în incaperi securizate. PMV este conectată la Internet prin Telecom și Serviciul de Telecomunicații Speciale. Infrastructura IT a PMV este prezentată în Anexa nr. 1.

5.3.4.1.2. Aplicații Software

Aplicațiile software standard ale MS Office sunt folosite pentru procesarea textelor, a foilor de calcul, prezentărilor, etc., în plus se utilizează și alte aplicații software - open source - sau aplicații software dedicate realizate de firme externe.

5.3.4.1.3. Resurse informaționale:

- bazele de date centrale de pe servere interne;
- bazele de date centrale aflate pe servere externe;
- datele locale de pe statiile de lucru ale utilizatorilor;
- manuale, proceduri de sistem, proceduri operaționale, ghiduri, regulamente, norme, reglementări aflate în format electronic și/sau format hârtie:
- contracte, facturi, oferte aflate în format electronic și/sau format hârtie:
- diverse alte documente (aprobări, autorizații, licențe) aflate în format electronic și/sau format hârtie.

5.3.4.2. Resurse umane

Conform ROF și fișelor de post.

5.3.4.3.Resurse financiare

Sunt asigurate conform Bugetului de venituri și cheltuieli al PMV.

5.4 Proiectarea, instalarea și administrarea infrastructurii de rețea

BIT proiectează, instalează și intreține infrastructura de rețea de calculatoare care deservește activitățile PMV:

5.4.1. Stabilirea elementelor rețelei:

1. Sistemele/subsistemele existente în PMV, care se bazează pe funcționarea rețelei sunt identificate cu rigurozitate;
2. Sistemele/subsistemele identificate pot fi configurate și supravegheate individual, folosind proceduri specifice
3. Sistemele/subsistemele identificate sunt utilizate conform specificațiilor tehnice ale producătorilor
4. Arhitectura de rețea aleasă, conectarea componentelor în rețea, distribuirea și configurarea serviciilor conduc la creșterea productivitatii muncii în organizație, la creșterea atractivității locului de munca;
5. Numarul componentelor de tip server și al celor de tip client se stabilește în conformitate cu activitățile desfașurate în PMV și cu soluțiile IT folosite;
6. Serverele și stațiile client sunt plasate în rețea și configurate conform regulilor impuse prin strategia de securitate implementată în instițutie.

5.4.2. Asigură buna funcționare a sistemelor/subsistemelor IT bazate pe existența și funcționarea rețelei de calculatoare:

1. Solutiile alese trebuie să respecte standardele în vigoare și specificațiile tehnice ale producătorilor
2. Soluțiile alese trebuie atent verificate și corectate, astfel încât aplicarea lor să conducă întotdeauna la obținerea de rezultate corecte și sigure;
3. Regulile, soluțiile tehnice și procedurile stabilite și folosite pentru replicarea/ dublicarea componentelor hardware, a serviciilor, aplicațiilor critice ale sistemelor/subsistemelor asigură funcționarea corectă, sigură și fără riscuri a sistemelor/subsistemelor IT;
4. Riscul apariției erorilor previzibile este corect evaluat;
5. Soluțiile ce vizează eliminarea sau atenuarea riscurilor, eliminarea erorilor previzibile sunt riguros aplicate;
6. La aparitia unor incidente neprevăzute se pun în practică proceduri de raspuns special construite.

5.4.3. Asigura și verifica utilizarea corectă și sigură a componentelor rețelei de către personalul PMV:

1. Regulile stabilite și implementate asigură accesul controlat și sigur al utilizatorilor numai la acele resurse de care au nevoie pentru îndeplinirea sarcinilor de serviciu conform fișei postului;
2. Datele/informațiile disponibile și folosite în rețea sunt întotdeauna corecte, sigure și sunt obținute la timp;
3. Regulile stabilite și implementate pentru urmărirea traficului de informații din rețea, a incărcării rețelei, a performanțelor serverelor și serviciilor sunt folosite

numai pentru evaluarea corectă a stării de funcționare a rețelei și a componentelor ei;
4. Dezvoltă, adaptează sau reconfigurează rețeaua pe baza evaluării modului de funcționare cu scopul creșterii performanțelor serviciilor, diminuării încărcării rețelei, respectiv diminuării traficului de date din rețea.

5.5 Asigurarea funcționalității rețelei de calculatoare și a echipamentelor de conectare și de comunicații

BIT are competență necesară pentru stabilirea de soluții, proceduri, tehnici pentru buna funcționare și corecta utilizare a echipamentelor de comunicații. Se includ aici procedurile și tehnicile de monitorizare și supraveghere impreuna cu cele de raspuns la aparitia unui incident. Urmarirea pe termen lung a performanțelor va fi vazută ca un instrument pentru optimizarea funcționarii sistemelor, subsistemelor și aplicațiilor, ca un mijloc de preintampinare și/sau detectare din timp a erorilor de funcționare.

5.5.1 Monitorizarea funcționarii rețelei se realizeaza prin:

1. Lista parametrilor de referință/control și valorile etalon folosite pentru evaluarea performanțelor echipamentelor hardware și ale componentelor software respecta specificațiile producătorilor și se incadrează în standarde;
2. Fiecare echipament și fiecare resursa monitorizată sunt caracterizate prin setul propriu de parametrii și valori acceptate, conform standardelor de funcționare și specificațiilor producatorului;
3. Momentele de timp, regulile și procedurile stabilite pentru supravegherea și colectarea valorilor parametrilor de referință nu afecteaza lucrul utilizatorilor și nici funcționearea sigură a sistemelor/subsistemelor/serviciilor/aplicațiilor;
4. Regulile, procedurile și criteriile folosite pentru evaluarea performanțelor nu conduc la ambiguități și identifică din timp posibilitatea apariției unor erori de funcționare;
5. Jurnalele cu valori măsurate ale parametrilor de referință/control vor fi pastrate și analizate periodic, în vederea stabilirii corecțiilor suplimentare pentru preintampinarea apariței erorilor de funcționare;
6. Jurnalele de evenimente sunt analizate periodic din punct de vedere statistic și tehnic pentru evaluarea punctelor slabe;
7. Punctele slabe, critice, limitările curente sunt eliminate prin folosirea remediilor stabilite conform specificațiilor tehnice ale producătorilor, echipamentelor hardware și ale produselor software;
8. Auditul resurselor folosite de utlizatori este folosit numai în scopul identificării și preintâmpinării breșelor de securitate și respectă legile în vigoare.

5.5.2 Detectarea nefuncționalităților hardware și software

1. Pentru evenimentele semnificative, erori, nefuncționalități hard și soft există proceduri stabilite executate de BIT;
2. Evenimentele, erorile, nefuncționalitățile pentru care exista proceduri standard de remediare sunt evaluat și se elaborează soluții de remediere;
3. Vulnerabilitațile identificate sunt corectate cu promptitudine.

5.5.3 Stabilirea parametrilor etalon

1. Fiecare componentă monitorizată este evaluată conform etalonului propriu;
2. Fiecare etalon este revizuit riguros în cazul reconfigurării infrastructurii de rețea;
3. Fiecare etalon este revizuit cu atenție în cazul modificărilor soluției generale IT;
4. La baza stabilirii parametrilor etalon stau caracteristicilor tehnice și de funcționare ale echipamentelor.

5.6 Administrarea serverelor

BIR instaleaza configureaza și intretine hardware și software serverele.

5.6.1 Instalarea , configurarea și administrarea echipamentelor hardware ale serverului

1. Resursele hardware instalate respectă indicațiile fabricantului;
2. Resursele hardware instalate și configurate respectă cerințele soluției IT implementate în instituție;
3. Accesul și utilizarea resurselor serverului respecăa strategia de securitate a rețelei;
4. Pentru resursele hardware critice este asigurată redundanța sau replicarea.

5.6.2 Instalarea, configurarea și administrarea serviciilor

1. Serviciile sunt instalate și configurate conform specificațiilor elaboratorilor;
2. Permisiunile de administrare sunt acordate numai personalului calificat și cu respectarea strategiei de securitate a rețelei;
3. Administrarea serviciilor se face de la distanță folosind instrumente specifice;
4. Soluțiile de salvare /restaurare și/sau redundanță a informațiilor sunt corecte și eficiente

5.6.3 Supravegherea utilizarii serviciilor

1. Jurnalele obtinute prin monitorizarea serviciilor sunt păstrate pentru a fi periodic consultate;
2. Jurnalele identifică utilizatorii care au avut acces la serviciu, în limita permisiunilor ce le-au fost acordate
3. Jurnalele identifică tentativele nereusite ale utilizatorilor de a avea acceas la servicii

4. Intrușii și atacatorii din interior și exterior pot fi identificați prin informațiile păstrate în jurnale

5.7 Interconectarea rețelelor și accesul la rețeaua globală Internet

BIT are compentența necesară pentru asigurarea accesului personalului din PMV la resurse aflate în afara rețelei locale, inclusiv în rețeaua Internet

5.7.1 Proiectează soluția de intercontare a rețelelor

1. Conexsiunile dintre rețele sunt conforme cu arhitecturile rețelelor și respectă standardele de interconectare;
2. Componentele hardware și software ale echipamentelor de legatură sunt configurate respenctând regulile de securitate a transmisiilor de date din strategia de securitate a institutiei
3. Tabelele de rutare sunt corect configurate și indică adresele rețelelor accesibile

5.7.2 Implementează soluția de interconectare

1. Instalarea și configurarea echipamentelor de legatură intre rețele respecă instrucțiunile din documentația tehnica a fabricantului;
2. Instalarea și configurarea componentelor software respectă indicațiile elaboratorilor și sunt conforme strategiei de securitate a institutiei;
3. Instalarea și configurarea produselor de tip „firewall" permite accesul în deplină siguranță la resursele rețelelor interconectate;
4. Filtrele asociate prin procedurile de tip „firewall" respectă strategia de securitate a instituției.

5.7.3 Proiectează și realizează conectarea la rețeaua Internet

1. Cerințele de conectare la Internet sunt identificate în conformitate cu fișa postului pentru fiecare categorie de personal și respectă strategie de securitate a instituției;
2. Accesul permis în rețeaua Internet la serviciile și serverele organizației este corect identificat și respectă strategia privitoare la accesul la informațiile instituției;
3. Colaborează cu organizațiile specializate pentru stablilirea conexiunilor la Internet;
4. Realizează conectarea la Internet în conformitate cu standardele în vigoare și specificațiile organizațiilor specializate;
5. Implementează regulile de securitate pentru accesul la și din rețeaua Internet în conformitate cu strategia de securitate a institutiei.

5.7.4 Monitorizează accesul la serviciile locale

1. Accesul la Internet la servicii este strict monitorizat pentru detectarea intrușilor și identificarea „atacatorilor";
2. Jurnalele sunt pastrate și analizate periodic din punct de vedere statistic
3. Detectarea intrușilor și a „atacatorilor" este urmată de executatea procedurilor predefinite conform strategiei de securitate

5.8. Proiectarea și aplicarea strategiei de securitate

5.8.1. Securitate IT - obiective

Punctul de plecare al oricarui model de securitate este asigurarea ca standardele și politicile de securitate își indeplinesc rolul de a proteja sistemele IT de atacurile externe și de folosirea neautorizată a resurselor PMV. Securizarea sistemului presupune implementarea unui set de proceduri, practici și tehnologii care au rolul de a proteja infrastructura IT cât și componența software și datele asociate acesteia. Obiectivul acestui capitol este de a asigura aceasta securitate hardware, software și a datelor din cadrul PMV.

5.8.2. Proceduri de securitate IT

Procedurile de securitate se impart în fizice, hardware, software și de comunicare și securitatea informației. Modalitatea detaliată de asigurare a securitatii IT este prezentată în Planul de securitate informatică al PMV. Aceste reguli sunt menținute de către personalul BIT al PMV împreună cu experții cu atributii IT ai PMV.

5.8.2.1. Securitate fizică

Securitatea fizică descrie măsurile care impiedică sau inlatură eventualii atacatori să acceseze facilitațile, resursele sau informațiile salvate pe surse externe. Securitatea fizică poate reprezenta diverse aspecte, de la o ușa incuiată la posturi multiple de gărzi.

Locația surselor, a echipamentului IT și a echipamentului subsidiar

- Echipamentele IT se gasesc în sediul PMV din Str. Spiru Haret Nr. 2, Vaslui, intr-o clădire care beneficiază de paăa permanentă, ca și la sediul SCPLEP.
- Echipamentul IT este distribuit personalului și se afla în camere cu acces limitat. Usile sunt inchise la sfarșitul zilei și doar personalul autorizat are acces.
- Toate serverele (file-serverul și webserverul) trebuie sa fie într-o camera sigură cu acces restricționat.
- Componentele de rețea (switch-uri) se afla în același loc cu serverele. Experții cu atribuții IT impreună cu BIT sunt responsabili de această camera.
- Toate liniile de curent și telecomununicații către sistemul informational sunt inchise în sigurantă.

Controlul accesului

• Accesul sediu se face pe bază de legitimație, PMV este pazită 24 ore din 24.

• Doar personalul autorizat are acces la camerele calculatoarelor.

• Vizitatorii trebuie sa fie insoțiți în timpul vizitelor în interiorul PMV. Personalul care a părăsit instituția sau care a fost suspendat nu are dreptul sa intre în interiorul PMV.

La sfarșitul fiecarei zlle, camerele sunt încuiate și numai personalul autorizat are acces la chei.

5.8.2.2. Securitatea Hardware

Securitatea hardware descrie procedurile necesare pentru a se asigura ca toate echipamentele electronice sunt sigure și ca doar personalul autorizat are acces la aceste echipamente.

Administrarea Securitatii Hardware

Responsabilitatea administrarii securitatii hardware depinde de echipamente și este distribuită dupa cum urrneaza:

• Fiecare utilizator este responsabil de propria stație de lucru.

• experții cu atribuții IT împreună cu BIT sunt responsabili de depozitarea și funcționarea echipamentelor IT în camera serverelor.

Intretinerea hardware

• Fiecare stație de lucru din cadrul PMV trebuie sa fie inventariată.

•Toate echipamentele importante trebuie intreținute în conformitate cu recomandările furnizorului în ceea ce privește service-ul și cu alte speciflcații ale acestuia.

•Doar personalul autorizat cu intreținerea poate desfășura activități de intreținere și service al echipamentelor, in masura competentelor.

•In cazul în care un angajat cere echipament IT aditional, atunci trebuie urmate procedurile corecte de achizitie.

5.8.2.3. Securitate Software

Asigurarea securitatii software inseamnă vulnerabilitate scazută, o mai mare eficiență operațională și siguranță ca aplicațiile software importante sunt cu adevarat sigure.

- Personalul nu este autorizat sa instaleze nici un fel de aplicație software;
- În cazul în care un angajat cere aplicații software adiționale, atunci trebuie urmate procedurile corecte de achiziție:
- BIT trebuie sa se asigure ca aplicațiile software anti-virus standard sunt instalate pe fiecare calculator din cadrul PMV;
- Personalul nu va indeparta sau dezactiva aplicatia software antivirus sau orice

altă aplicație software din calculator;

- Doar experți cu atributii IT sau BIT pot instala aplicații software sau dezactiva aplicațiile software care nu sunt utilizate.
- Numai BIT pot intreprinde măsurile necesare pentru îndepartarea download-arilor neautorizate de aplicații software;
- Toți utilizatorii trebuie să respecte înțelegerile de respectare a legii dreptului de autor și a acordurilor asupra licenței software;
- Upload-area și download-area materialului protejat de drepturile de autor este interzisă.
  Afișarea materialului protejat de legile dreptului de autor pe serverele de intranet sau internet (servere plasate în interiorul rețelei) este de asemenea strict interzisă
- Personalul nu poate partaja informațiile și datele confidentiale din propria stație de lucru;

5.8.2.4. Securitatea Comunicarii

Administrarea comunicării și caracteristicile siguranței

- Comunicațiile interne și externe se bazează pe poșta electronică și portalul website.
- Experții cu atribuții IT, în colaborare cu BIT, sunt responsabili de crearea și intreținerea conturilor de poștă electronică, dar fiecare angajat are responsabilitatea propriei poște electronice
- Nu este nici o problema în ceea ce priveste securitatea postei electronice datorita aplicației software instalate pe server. În cazul în care un mesaj electronic conține viruși, acesta va fi în mod automat blocat și nu va fi lăsat să se transmită mai departe către exterior.
- Personalul:
  - Nu va dezactiva sau indeparta aplicațiile software de pe calculatoare.
  - Nu va deschide fișiere sau macro atașate la un mesaj electronic provenind dintr-o sursa necunoscută, suspectă sau care nu prezintă incredere și va șterge imediat aceste atașamente, apoi le va șterge din nou prin golirea Coșului de reciclare.

Software pentru Comunicare

- Personalul nu are dreptul de a partaja informația clasificată sau confidențială de pe propria stație de lucru. Utilizatorul poate partaja sau transfera date folosind:
  - Portalul website
  - Serverul de poștă electronică

Protejarea informațiilor în mediul de comunicare

- Aplicația software anti-virus a PMV trebuie sa fie instalată pe fiecare stație de lucru;

Administrarea securitatii datelor

In vederea atingerii obiectivelor operaționale, PMV se bazează pe sistemele de procesare electronică a datelor și pe datele conținute de acestea. Este esențial ca aceste sisteme să fie protejate de folosirea greșita și atât sistemele computerizate cât și toate datele să fie accesate și menținute într-un mediu sigur. Aceasta secțiune și anexele aferente descriu măsurile întreprinse pentru asigurarea confidențialității și integrității informațiilor și în plus, măsurile necesare protejării datelor de accesările neautorizate.

Administrarea securitatii datelor

- Fiecare angajat este responsabil de datele din calculatorul propriu.
- Fiecare cont de poștă electronică are un nume și o parolă cunoscute doar de persoana care deține contul respectiv și de BIT
- Toate parolele de la nivelul sistemului sunt administrate și controlate de expertil IT și BIT PMV, din interiorul clădirii unde funcționează PMV;
- Toate parolele de utilizator sunt schimbate cel puțin o dată la șase luni sau ori de cate ori acestea sunt compromise;
- Toate parolele de utilizator și celelalte parole trebuie sa fie conforme.

5.8.2.5. Politico Anti-virus

Existența unei politici conform careia trebuie luate măsuri pentru protejarea calculatoarelor, serverelor și a datelor de viruși este vitaăa. Există mai multe tipuri de viruși care pot cauza defecțiuni serioase la nivelul computerului.

- experții cu atribuții IT, în colaborare cu BIT, se asigură că există aplicația software anti-virus pe fiecare computer din cadrul PMV;
- experții cu atribuții IT, în colaborare cu BIT, se asigură că ultima versiune a aplicației software anti-virus este instalată și că fișierele de definire a virusului sunt aduse la zi. Aceste fișiere trebuie verificate și înnoite cel puțin o data pe saptămână.
- BIT vor furniza o informare regulată și instruire personalului PMV asupra politicii anti-virus;
- personalul PMV:
  - nu va îndeparta aplicația software anti-virus de pe nici un computer;
  - nu va deschide fișiere sau macro atașate la un mesaj electronic care provine dintr-o sursa necunoscută, suspectă sau care nu prezintă încredere și va șterge aceste atașamente imediat, apoi le va șterge din nou din cadrul coșului de reciciare. În cazul în care aveti întrebări, contactați BIT;
  - va sterge mesajele electronice spam, lanțurile de mesaje sau alte mesaje

publicitare fara a le redirectiona
- nu va descarca fișiere care provin din surse necunoscute sau suspecte;
- va evita partajarea directă în care există drepturi de scriere sau citire atât timp cât nu este necesară

- este posibil ca personalul PMV sa primească uneori mesaje electronice din partea unor prieteni, colegi sau alte surse care îi avertizeaza cu privire la apariția unui nou virus sau atașamente la mesajele electronice care pot cauza daune computerului. Aceste avertizări citează în general surse credibile și recornandă de obicei ca cel care primește mesajul să-l trimită mai departe cunoștințelor. Uneori aceste mesaje sfătulesc persoana care primește să șteargă anumite fișlere din computer. Deseori aceste avertizari sunt doar niște farse și deși sunt mai puțin periculoase decât virușii reali să consume totusi resurse, incarcă memoria casuțelor de poștă electronică și în cel mai rău caz utilizatorii, în urma sfaturilor primite, pot șterge anumite fișiere din memorie. În cazul în care o persoană primește astfel de avertismente aeesta nu trebuie să trimită mai departe sau să urmeze instrucțiunile incluse în mesaj. Utilizatorul trebuie să contacteze personalul specializat care sa investigheze problema și va sfatui utilizatorii asupra măsurilor care se impun.

5.8.3. Securitate și confidențiatitate

- Toti utilizatorii serviciilor de poștă electronics trebuie sa ia masurile necesare pentru a proteja confidențialitatea mesajelor electronice sau a oricaror inregistrări care conțin informații personale și confidențiale pe care le-au întâlnit în timpul desfășurării sarcinilor de serviciu sau în orice alt mod.
- In consecință, conturile de poștă electronică pot fi accesate doar prin intermediul unei parole. În afara de BIT, doar posesorul contului de email cunoaste parola respectivă.
- Securitatea fizica și electronică a serverului de posts electronica este responsabilitatea firmei care asigura accesul la internet, Telecom asigurand configurarea, administrarea și mentenanța acestuia.

5.8.4. Recuperarea datelor în caz de dezastru

In aceasta sectiune se vor face referiri la procedeele de recuperare a datelor în timp scurt și cu pierderi minime. Atunci când un calculator se defecteaăa, se intrerupe alimentarea cu energie electrică sau intervin alte dezastre, PMV trebuie sa puna în practică un set de proceduri dinainte stabilite. Este important ca PMV sa dețină procedurile necesare rezolvarii acestor situatil critice.

Obiectivul principal este de a ajuta PMV sa supraviețuiască unui dezastru și să restabilească operațiunile normale.

Pentru a supraviețui, trebuie să se asigure ca operațiile importante pot reveni la normal în scurt timp. De aceea PMV trebuie să:

- Identifice punctele slabe și să implementeze un program de prevenire a dezastrelor;
- Să minimalizeze durata intreruperilor serioase ale activității;
- Să faciliteze coordonarea sarcinilor de recuperare;
- Să reducă complexitatea efortului de recuperare.

Pentru a preveni astfel de situații se impune realizarea activităților de back-up și restaurare destinata migrării efectelor situatiei de urgență.

Salvarea Datelor

- Utilizatorii sunt responsabili de propriile date, astfel încât vor realiza back-up-uri periodice pe unul din suporturile puse la dispozitie. Datele trebuie stocate pe suporturi sigure. Toate datele trebuie clasificate în funcție de importanța în cadrul PMV și salvarea datelor se face în mod corect;
  - Mediile de stocare trebuie etichetate cu informațiile următoare:
  - Salvarea datelor
  - Continutul salvarii datelor.
- In cazul în care PMV va considera necesară existenta unui server de partajare a fișierelor, fiecare utilizator poate salva fișiere pe acest server și este responsabil de integritatea datelor;
- Procedurile de salvare a datelor trebuie sa fie în concordantă cu prevederile în domeniul informatic referitoare la protejarea datelor critice pentru o organizație.

CD-urile cu software și cele cu backup de date vor fi pastrate intr-un spatiu sigur, un seif sau dulap . BIT sunt singurele persoane care au acces la camera sau dulapul în care sunt depozitate CD cu soft sau cu datele salvate. Se creaza copii ale CD-urilor cu software atunci când este necesar.

Restaurarea datelor

In caz de dezastru sau când e necesară o reinstalare a sistemului de operare, datele vor fi restaurate folosind cea mai recenta versiune a backup-ului efectuat.

6. RESPONSABILITĂȚI

6.1 BIT

Sarcini:

1. Coordonarea activității de informatică și de a efectua tranzacțiile pentru prelucarea automată a datelor
2. Pentru protecția anumitor date sau documente împotriva pierderilor voite sau accidentale,accesul în sistemul automat de evidența și prelucare a acestor date este controlat prin parola și nivel de acces

a) Folosirea aplicației software, în conformitate cu instrucțiunile scrise de programatori;
b) Sesizarea și corectarea erorilor semnalate în timpul rulării programului;
c) Pentru a evita pierderea sau distrugerea datelor, cel puțin anual, se salvează toate fișierele și programele pe un hard special, folosit numai în acest scop, la fiecare compartiment;

3. Anual intocmește lista cu programe utilizate, continând:
   a) Denumirea programnului;
   b) Furnizoru;
   c) Date de identificare sau reprezentantul;
   d) Alte date necesare utilizarii (contract,regulament,etc...)
4. Instalează și intretine pe calculatoare din rețea software în acord cu contractele de licențiere
5. Asigură securitatea rețelei administrate, previne și rezolvă situațiile de virusare a calculatoarelor din rețea;
6. Intreține și administrează rețeaua de calculatoare;
7. Intervine prompt în localizarea, izolarea și remedierea unor defecțiuni în reațea, restaurează, in masura competentelor, funcționarea rețelei la parametrii maximi permiși de defecțiunea respectivă, rețeaua fiind în stare de funcționare la parametrii optimi;
8. Împreună cu furnizorii de echipamente de calcul urmarește depanarea hardware a echipamentelor defecte;
9. Instalează în rețea, în colaborare cu furnizorii, dispozitive periferice specice: scanere, imprimante, multifuncționale, etc.;
10. Elaboreaza specificațiile tehnice specifice necesare întocmirii caietelor de sarcini pentru achizițiile de tehnică de calcul;
11. Sunt raspunzători de compatibilitatea echipamentelor achiziționate cu cele existente;
12. Consiliază și asistă personaul din cadrul primariei cu privire la utilizarea software-lui destinat aplicațiilor locale, dar și a celui specific serviciilor Internet;
13. Asigură asistenta software pentru aplicațiile existente sau pentru cele noi achiziționate, în masură compențelor, dacă nu contactează firmele specializate sau persoanele autorizate care au realizat aplicațiile respective.
14. Asistă personalul la utilizarea diferitelor programe, deja instalate și functionale
15. Asigura legatura între firmele și persoanele autorizate, care au realizat anumite aplicații utilizate în cadrul primăriei și personalul care le utilizează
16. Asigură arhivarea în sistem informatic a datelor din cadrul PMV, cu respectarea normelor legale în vigoare.

7. ANEXE

Nu este cazul.

8. DIAGRAMA DE PROCES PENTRU SOLICITARI DE DOTARI HARDWARE/ FOSTWARE