PROGRAMUL OPERAȚIONAL PENTRU PESCUIT ȘI AFACERI MARITIME 2014-2020

MANUAL DE PROCEDURĂ PENTRU TEHNOLOGIA INFORMAȚIEI

cod manual: M04-e.I.r.0

1. Lista responsabililor cu elaborarea, verificarea şi aprobarea ediţiei sau, după caz, a reviziei în cadrul ediţiei procedurii operaţionale

	Tipul acţiunii	Nume şi prenume	Funcţia / Compartiment	Semnătura/ Data
1.1	Elaborat	**Alina ALEXE**	Consilier SPMM	22.06.2016
1.2	Verificat	**Eduard DIACONEASA**	Şef serviciu SPMM	22.06.2016
1.3	Aprobat	**Ciceronis CUMPĂNĂŞOIU**	Director general DGP-AMPOP	

2. Situaţia ediţiilor şi a reviziilor în cadrul ediţiilor procedurii operaţionale

	Ediţia sau, după caz, revizia în cadrul ediţiei	Capitol/anexă revizuit/ă	Modalitatea reviziei (M=modificare, A=adăugare, S=suprimare)	Data de la care se aplică prevederile ediţiei sau reviziei ediţiei
2.1	Ediţia I			

3. Lista cuprinzând persoanele la care se difuzează ediţia sau, după caz, revizia din cadrul ediţiei procedurii operaţionale

Documentul scanat se distribuie întregului personal, conform statului de funcţii al DGP-AMPOPAM. Comunicarea documentului către personalul DGP-AMPOPAM se efectuează prin intermediul poştei electronice.
Personalul DGP-AMPOPAM are obligaţia de a salva şi stoca, în format electronic, pe staţia de lucru, procedura operaţională primită prin poşta electronică.

4. Scop

Prin această procedură, DGP-AMPOPAM:

4.1. Stabileşte modul de realizare a activităţii, compartimentele şi persoanele implicate.

4.2. Asigură continuitatea activităţilor, incluzând planul de acţiune în caz de dezastru.

4.3 Sprijină auditul şi/ sau alte organisme abilitate în acţiuni de auditare şi/ sau control, iar pe manager, în luarea deciziei.

4.4 Creează şi menţine o infrastructură de management informaţional care presupune o interacţiune între oameni (utilizatori şi Specialişti IT), tehnologie (hardware, software şi reţele) şi procese (modul în care oamenii şi sistemele interacţionează). Această interacţiune presupune monitorizare zilnică şi ajustări permanente pentru a crea sinergia şi eficienţa maximă. Pentru a susţine administrarea acestei activităţi complexe, procedurile sunt stabilite în cadrul unui Plan de securitate informatică şi un Plan de Recuperare în caz de dezastru.

Acest document descrie următoarele elemente necesare administrării informaţiei în cadrul DGP-AMPOPAM :

- infrastructura IT şi organizarea acesteia în cadrul DGP-AMPOPAM;

- planul de securitate informatică, care se referă la resursele, aplicaţiile şi alte date ca parte integrantă a administrării infrastructurii informaţionale şi securizarea organizaţiei în viitor. Securizarea unui sistem presupune implementarea unui set de proceduri, reguli şi tehnologii pentru a proteja infrastructura IT cât şi a datelor din cadrul organizaţiei. Atunci când calculatoarele se defectează, ori este întreruptă alimentarea cu energie sau se întamplă anumite dezastre, trebuie puse în aplicare un set de proceduri şi procese.

- modalitatea de recuperare în cazul apariţiei unui dezastru care poate distruge infrastructura de comunicaţii.

Capitolele sunt prezentate pe scurt fără a conţine proceduri detaliate de lucru. Procedurile detaliate, cum ar fi salvarea şi refacerea datelor, regulile de securitate se schimbă frecvent şi prin urmare acestea au fost scrise în anexe separate.

5. Domeniu de aplicare

Prezenta procedură operaţională vine în completarea Planului de securitate informatică al MADR şi va fi aplicată pentru toate activităţile realizate de personalul DGP-AMPOPAM.

6. Documente de referinţă (reglementări internaţionale şi naţionale)

6.1. Legislaţie UE

- **Regulamentul (UE) nr. 508/2014** privind Fondul european pentru pescuit şi afaceri maritime şi de abrogare a Regulamentelor (CE) nr. 2328/2003, (CE) nr. 861/2006, (CE) nr. 1198/2006 şi (CE) nr. 791/2007 ale Consiliului şi a Regulamentului (UE) nr. 1255/2011 al Parlamentului European şi al Consiliului
- **Regulamentul (UE) NR nr 1303/2013** de stabilire a unor dispoziţii comune privind Fondul european de dezvoltare regională, Fondul social european, Fondul de coeziune, Fondul european agricol pentru dezvoltare rurală şi Fondul european pentru pescuit şi afaceri maritime, precum şi de stabilire a unor dispoziţii generale privind Fondul european de dezvoltare regională, Fondul social european, Fondul de coeziune şi Fondul european pentru pescuit şi afaceri maritime şi de abrogare a Regulamentului (CE) nr. 1083/2006 al Consiliului.

6.2. Legislaţie naţională

- **HG nr. 58/1998** pentru aprobarea Strategiei naţionale de informatizare şi implementare în ritm accelerat a societăţii informaţionale şi a Programului de acţiuni privind utilizarea pe scară largă şi dezvoltarea sectorului tehnologiilor informaţiei in Romania;
- **OG nr. 25/2006** privind întărirea capacităţii administrative a Oficiului Român pentru Drepturile de Autori, republicată, cu modificările şi completările ulterioare;
- **Legea nr. 64/2004** pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2011;
- **HG nr. 1185/2014** privind organizarea şi funcţionarea Ministerului Agriculturii şi Dezvoltării Rurale, cu modificările şi completările ulterioare.

7. Definiţii şi abrevieri ale termenilor utilizaţi în procedura operaţională

7.1. Definiţii ale termenilor:

Nr. crt.	Termenul	Definiţia
1	Circumstanţe care depind de timp şi operaţii operaţiunilor critice	Circumstanţe când întârzierea acţiunii poate împiedica DGP-AMPOPAM să îşi atingă scopurile şi obiectivele strategice.
2	Circumstanţe de urgenţă	circumstanţele în care timpul este esenţial şi există o mare probabilitate ca întârzierea situaţiei să determine o agravare a situaţiei.
3	Folosire a serviciilor de poştă electronică ale DGP-AMPOPAM	crearea, trimiterea, redirecţionarea, transmiterea, salvarea, păstrarea, copierea, descărcarea, citirea sau tipărirea mesajelor electronice (cu ajutorul serviciilor de poştă electronică ale DGP-AMPOPAM). Un utilizator al poştei electronice este o persoană care foloseşte serviciile poştei electronice a DGP-AMPOPAM.
4	Poştă electronică	una sau mai multe înregistrari computerizate sau mesaje create, trimise, redirecţionate, publicate, citite, văzute sau tipărite de către unul sau mai multe sisteme sau servicii de poştă electronică. Această definiţie a înregistrărilor mesajelor electronice se aplică întregului conţinut al acestor înregistrări şi informaţiilor asociate cu aceste înregistrări, cum ar fi header, sumar, adrese şi destinatari.
5	Sisteme sau servicii de poştă electronică	orice sistem de trimitere a mesajelor care are la baza un sistem computerizat pentru crearea, trimiterea, înaintarea, răspunderea transmiterea, înmagazinarea, oprirea, copierea, descărcarea, citirea sau printarea înregistrărilor computerizate în scopul unei comunicări între reţele computerizate sau între indivizi sau grupuri, care în mod explicit indică un sistem de poştă electronică sau este folosit explicit pentru alte scopuri, inclusiv servicii cum ar fi buletine electronice de mesaje, liste cu servere sau grupuri de ştiri.

7.2. Abrevieri ale termenilor

Nr. crt.	Abrevierea	Termenul abreviat
1	DGP-AMPOPAM	Direcţia generală Autoritatea de management pentru POPAM
2	CIT	Compartimentul IT MADR
3	FEPAM	Fondul European pentru Pescuit și Afaceri Maritime
4	MADR	Ministerul Agriculturii şi Dezvoltării Rurale
5	MFE	Ministerul Fondurilor Europene
6	ROF	Regulamentul de Organizare și Funcționare al MADR
7	RL	Reţea locală

8. Descrierea activităţii

8.1. Generalităţi

În vederea desfăşurării activităţilor stabilite prin ROF, DGP-AMPOPAM depinde de infrastructura computerizată. În continuare este prezentată o descriere a organizării informaţiei şi a infrastructurii tehnice.

8.2. Documente utilizate

8.2.1. Lista şi proveniența documentelor utilizate

Nr.crt.	Denumire	Proveniență
1	Planul de securitate informatică al MADR	CIT
2	Ordin al ministrului agriculturii şi dezvoltării rurale de numire/eliberare în/din funcţie	structura cu competențe de resurse umane din MADR
3	Decizie a directorului general al DGP-AMPOPAM	DGP-AMPOPAM
4	Solicitare scrisă a conducătorului unei structuri externe	Structura externă
5	Procedura operațională Activarea unui cont de utilizator al Aplicațiilor 2014, PO-DITCS.01	MFE
6	Declaraţie de confidenţialitate şi imparţialitate	DGP-AMPOPAM

8.2.2. Conținutul și rolul documentelor utilizate

Rolul Planului de securitate informatică al MADR este acela de a stabili practici prudente și acceptabile privind utilizarea sistemului informatic al MADR. Acest document descrie activitățile sistemului ce privesc securitatea bazate pe procedurile MADR și asigurarea conformității sistemului informatic cu standardul SR ISO/CEI 27002.

Prin Ordin al ministrului agriculturii şi dezvoltării rurale de numire/eliberare în/din funcție și/sau Decizie a directorului general al DGP-AMPOPAM se stabilesc atribuțiile personalului DGP-AMPOPAM, și astfel se pot identifica drepturile de acces în aplicația informatică SIMPOP.

Procedura operațională Activarea unui cont de utilizator al Aplicațiilor 2014 stabilește cadrul general și procedural unitar privind acordarea drepturilor de acces în cadrul Aplicațiilor 2014 gestionate de Ministerul Fondurilor Europene (MySMIS2014, SMIS2014 etc.). Această procedură va fi aplicată de tot personalul DGP-AMPOPAM pentru a putea utiliza aceste aplicații.

Securitatea și confidențialitatea informațiilor

Toţi angajaţii DGP-AMPOPAM au obligaţia de a proteja confidenţialitatea informaţiilor pe care le-au întâlnit în timpul desfăşurării atribuţiunilor sau în orice alt mod. În acest sens, fiecare angajat al DGP-AMPOPAM va semna anual Anexa 1 - Declaraţie de confidenţialitate şi imparţialitate.

8.3. Resurse necesare

8.3.1. Resurse materiale

8.3.1.1. Hardware şi reţele

În cadrul DGP-AMPOPAM există un număr de 100 de calculatoare personale conectate într-o Reţea Locală din cadrul MADR. Sistemele operaţionale sunt pe platforma Windows. Există diferite servere în cadrul DGP-AMPOP. Aceste servere sunt situate toate într-o singură cameră. DGP-AMPOPAM este conectată la Internet prin Serviciul de Telecomunicaţii Speciale. Infrastructura IT a DGP-AMPOPAM este prezentată în Anexa nr. 2.

8.3.1.2. Aplicaţii Software

Aplicaţiile software standard ale MS Office sunt folosite pentru procesarea textelor, a foilor de calcul, prezentări, etc. În plus se utilizează şi alte aplicaţii software – open source – sau aplicaţii software dedicate. Acestea provin din surse externe cum ar fi Comisia Europeană, Ministerul Fondurilor Europene (Aplicaţiile 2014) sau au fost dezvoltate de parteneri privaţi *(SIMPOP – Sistemul Informatic pentru Managementul POP).*

8.3.1.3. Resurse informaţionale:

a. bazele de date centrale de pe servere interne;
b. bazele de date centrale aflate pe servere externe;
c. datele locale de pe staţiile de lucru ale utilizatorilor;
d. manuale, proceduri de sistem, proceduri operaţionale, ghiduri, regulamente, norme, reglementări aflate în format electronic şi/sau format hârtie;
e. contracte, facturi, oferte aflate în format electronic şi/sau format hârtie;
f. diverse alte documente (aprobări, autorizaţii, licenţe) aflate în format electronic şi/sau format hârtie.

8.3.2. Resurse umane

Conform ROF şi fişelor de post.

8.3.3. Resurse financiare

Sunt asigurate conform Bugetului de venituri şi cheltuieli al MADR precum şi prin intermediul POPAM 2014-2020.

8.4. Modul de lucru

8.4.1. Securitate IT - obiective

Punctul de plecare al oricărui model de securitate este asigurarea că standardele şi politicile de securitate îşi îndeplinesc rolul de a proteja sistemele IT de atacurile externe şi de folosirea neautorizată a resurselor DGP-AMPOPAM. Securizarea sistemului presupune implementarea unui set de proceduri, practici şi tehnologii care au rolul de a proteja infrastructura IT cât şi componenta software şi datele asociate acesteia. Obiectivul acestui capitol este de a asigura această securitate hardware, software şi a datelor din cadrul DGP-AMPOPAM.

8.4.2. Proceduri de securitate IT

Procedurile de securitate se împart în fizice, hardware, software şi de comunicare şi securitatea informaţiei. Modalitatea detaliată de asigurare a securităţii IT este prezentată în Planul de securitate informatică al MADR. Aceste reguli sunt menţinute de către Administratorul Reţelei IT a MADR împreună cu experţii cu atribuţii IT ai DGP-AMPOPAM.

8.4.2.1. Securitate fizică

Securitatea fizică descrie măsurile care împiedică sau înlătură eventualii atacatori să acceseze facilităţile, resursele sau informaţiile salvate pe surse externe. Securitatea fizică poate reprezenta diverse aspecte, de la o uşă încuiată la posturi multiple de gărzi.

Locaţia surselor, a echipamentului IT şi a echipamentului subsidiar

- Echipamentele IT se găsesc în sediul MADR din Bd. Carol I nr.2-4, sector 3, Bucureşti, într-o clădire care beneficiază de pază permanentă, ca și la sediile CRPOP.
- Echipamentul IT este distribuit personalului şi se află în camere cu acces limitat. Uşile sunt închise la sfârşitul zilei şi doar personalul autorizat are acces.
- Toate serverele (serverul de poştă electronică, file-serverul şi webserverul) trebuie să fie într-o cameră sigură cu acces restricţionat.
- Componentele de reţea (switch-uri) se află în acelaşi loc cu serverele. Experţii cu atribuţii IT împreună cu CIT sunt responsabili de această cameră.
- Toate liniile de curent şi telecomunicaţii către sistemul informaţional sunt închise în siguranţă.

Controlul accesului

- Accesul sediu se face pe bază de legitimaţie. DGP-AMPOPAM este păzită 24 ore din 24.
- Doar personalul autorizat are acces la camerele calculatoarelor.
- Vizitatorii trebuie să fie însoţiţi în timpul vizitelor în interiorul DGP-AMPOPAM.
- Personalul care a părăsit instituţia sau care a fost suspendat nu are dreptul să intre în interiorul DGP-AMPOPAM.
- La sfârşitul fiecărei zile, camerele sunt încuiate şi numai personalul autorizat are acces la chei.

8.4.2.2. Securitatea Hardware

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

Administrarea Securităţii Hardware

Responsabilitatea administrării securităţii hardware depinde de echipamente şi este distribuită după cum urmează:

- Fiecare utilizator este responsabil de propria staţie de lucru.
- Experţii cu atribuţii IT împreună cu CIT sunt responsabili de depozitarea şi funcţionarea echipamentelor IT în camera serverelor.

Întreţinerea hardware

- Fiecare staţie de lucru din cadrul DGP-AMPOPAM trebuie să fie inventariată.

- Toate echipamentele importante trebuie întreţinute în conformitate cu recomandările furnizorului în ceea ce priveşte service-ul şi cu alte specificaţii ale acestuia.
- Doar personalul autorizat cu întreţinerea poate desfăşura activităţi de întreţinere şi service al echipamentelor.
- În cazul în care un angajat cere echipament IT adiţional, atunci trebuie urmate procedurile corecte de achiziţie.

8.4.2.3. Securitate Software

Asigurarea securităţii software înseamnă vulnerabilitate scăzută, o mai mare eficienţă operaţională şi siguranţa că aplicaţiile software importante sunt cu adevărat sigure.

- Personalul nu este autorizat să instaleze nici un fel de aplicaţie software;
- În cazul în care un angajat cere aplicaţii software adiţionale, atunci trebuie urmate procedurile corecte de achiziţie;
- Experţii cu atribuţii IT împreună cu experţii CIT trebuie să se asigure că aplicaţiile software anti-virus standard sunt instalate pe fiecare calculator din cadrul DGP-AMPOPAM;
- Personalul nu va îndepărta sau dezactiva aplicaţia software antivirus sau orice altă aplicaţie software din calculator;
- Doar experţii cu atribuţii IT sau experţii CIT pot instala aplicaţii software sau dezactiva aplicaţiile software care nu sunt utilizate.
- Numai experţii cu atribuţii IT sau experţii CIT pot întreprinde măsurile necesare pentru îndepărtarea download-arilor neautorizate de aplicaţii software;
- Toţi utilizatorii trebuie să respecte înţelegerile de respectare a legii dreptului de autor şi a acordurilor asupra licenţei software;
- Uploadarea şi download-area materialului protejat de drepturile de autor este interzisă. Afişarea materialului protejat de legile dreptului de autor pe serverele de intranet sau internet (servere plasate în interiorul reţelei) este de asemenea strict interzisă;
- Personalul nu poate partaja informaţiile şi datele confidenţiale din propria staţie de lucru;

8.4.2.4. Securitatea Comunicării

Administrarea comunicării şi caracteristicile siguranţei

- Comunicaţiile interne şi externe se bazează pe telefon, poşta electronică şi portalul website.
- Experţii cu atribuţii IT, în colaborare cu CIT, sunt responsabili de crearea şi întreţinerea conturilor de poştă electronică, dar fiecare angajat are responsabilitatea propriei poşte electronice
- Nu este nici o problemă în ceea ce priveşte securitatea poştei electronice datorita aplicaţiei software instalate pe server. În cazul în care un mesaj electronic contine viruşi, acesta va fi în mod automat blocat şi nu va fi lasat sa se transmita mai departe catre exterior.
- Personalul:
  - Nu va dezactiva sau îndepărta aplicaţiile software de pe calculatoare.
  - Nu va deschide fişiere sau macro ataşate la un mesaj electronic provenind dintr-o sursă necunoscută, suspectă sau care nu prezintă încredere şi va şterge imediat aceste ataşamente, apoi le va şterge din nou prin golirea Coşului de reciclare.

Întreţinerea comunicării

- Există un contract de întreţinere cu un furnizor extern pentru centrala telefonică încheiat de MADR.
- CIT, în colaborare cu Serviciul de Telecomunicaţii Speciale, este responsabil de buna funcţionare a serverului de poştă electronică şi de conturile de poştă electronică.

Software pentru Comunicare

- Personalul nu are dreptul de a partaja informaţia clasificată sau confidenţială de pe propria staţie de lucru. Utilizatorul poate partaja sau transfera date folosind:
  - un server sigur de partajare a fişierelor
  - Portalul website
  - Serverul de poştă electronică

Protejarea informaţiilor în mediul de comunicare

- Protejarea împotriva intruşilor se face prin intermediul unui firewall.
- Aplicatia software anti-virus a DGP-AMPOPAM trebuie să fie instalată pe fiecare staţie de lucru cât şi pe serverul de poştă electronică.
- În cazul în care mesajul electronic conţine viruşi, acesta va fi în mod automat blocat de server.
- Serverul de poştă electronică trebuie să fie salvat corect şi să existe verificări periodice pentru a preveni ca personalul neautorizat să aibă acces la mesajele electronice ale celorlalţi.

8.4.2.5. Securitatea Datelor şi Informaţiei

În vederea atingerii obiectivelor operaţionale, DGP-AMPOPAM se bazează pe sistemele de procesare electronică a datelor şi pe datele conţinute de acestea. Este esenţial ca aceste sisteme să fie protejate de folosirea greşită şi atât sistemele computerizate cât şi toate datele să fie accesate şi menţinute într-un mediu sigur. Această secţiune şi anexele aferente descriu măsurile întreprinse pentru asigurarea confidenţialităţii şi integrităţii informaţiilor şi în plus, măsurile necesare protejării datelor de accesările neautorizate.

Administrarea securităţii datelor

- Fiecare angajat este responsabil de datele din calculatorul propriu.
- În cazul în care angajatul lipseşte mai mult de 10 minute, apare screensaver-ul care poate fi oprit prin introducerea numelui utilizatorului şi a parolei;
- Fiecare cont de poştă electronică are un nume şi o parolă cunoscute doar de persoana care deţine contul respectiv şi de experţii CIT;
- Toate parolele de la nivelul sistemului sunt administrate şi controlate de experţii CIT şi cei cu atribuţii IT din cadrul DGP-AMPOPAM, din interiorul clădirii unde funcţionează DGP-AMPOPAM;
- Toate parolele de utilizator sunt schimbate cel puţin o dată la şase luni sau ori de câte ori acestea sunt compromise;
- Toate parolele de utilizator şi celelalte parole trebuie să fie conforme.

Protejarea datelor în timpul transferării în reţele de date

- Reteaua locală trebuie să fie protejată de către un firewall.
- Pe server trebuie să fie instalat un program anti-virus.

8.4.2.6. Politica Anti–virus

Existenţa unei politici conform căreia trebuie luate măsuri pentru protejarea calculatoarelor, serverelor şi a datelor de viruşi este vitală. Există mai multe tipuri de viruşi care pot cauza defecţiuni serioase la nivelul computerului.

- experţii cu atribuţii IT, în colaborare cu CIT, se asigură că există aplicaţia software anti-virus pe fiecare computer din cadrul DGP-AMPOPAM;
- experţii cu atribuţii IT, în colaborare cu CIT, se asigură că ultima versiune a aplicaţiei software anti-virus este instalată şi că fişierele de definire a virusului sunt aduse la zi. Aceste fişiere trebuie verificate şi înnoite cel puţin o dată pe saptămână.
- experţii cu atribuţii IT vor furniza o informare regulată şi instruire personalului DGP-AMPOPAM asupra politicii anti-virus;
- personalul DGP-AMPOPAM:
  - nu va îndepărta aplicaţia software anti-virus de pe nici un computer;
  - nu va deschide fişiere sau macro ataşate la un mesaj electronic care provine dintr-o sursă necunoscută, suspectă sau care nu prezintă încredere şi va şterge aceste ataşamente imediat, apoi le va şterge din nou din cadrul coşului de reciclare. În cazul în care aveţi întrebări, contactaţi expertul IT;
  - va şterge mesajele electronice spam, lanţurile de mesaje sau alte mesaje publicitare fără a le redirecţiona;
  - nu va descărca fişiere 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 DGP-AMPOPAM să primeasca uneori mesaje electronice din partea unor prieteni, colegi sau alte surse care îi avertizează cu privire la apariţia unui nou virus sau ataşamente la mesajele electronice care pot cauza daune computerului. Aceste avertizări citează în general surse credibile şi recomandă de obicei ca cel care primeşte mesajul să-l trimită mai departe cunoştinţelor. Uneori aceste mesaje sfătuiesc persoana care îl primeşte să şteargă anumite fişiere din computer. Deseori aceste avertizări sunt doar nişte farse şi deşi sunt mai putin periculoase decât viruşii reali consumă totuşi resurse, încarcă memoria căsuţelor de poştă electronică şi în cel mai rău caz utilizatorii, în urma sfaturilor primite, pot şterge anumite fişiere din memorie. În cazul în care o persoană primeşte astfel de avertismente acesta nu trebuie să trimită mai departe sau să urmeze instrucţiunile incluse în mesaj. Utilizatorul trebuie să contacteze personalul specializat care va investiga problema şi va sfătui utilizatorii asupra măsurilor care se impun.

8.4.3. Poșta electronică

8.4.3.1. Politica Poştei electronice

DGP-AMPOPAM foloseşte poşta electronică pentru anumite anunţuri. Pentru atingerea nevoilor operaţionale DGP-AMPOPAM se bazează pe sistemul poştei electronice. Angajaţii trebuie să verifice căsuţele de poştă electronică în mod regulat.

Scopul acestei politici este de a asigura:

- informarea angajaţilor asupra ariei de aplicare a politicilor şi regulilor despre poşta electronică;
- serviciile de poştă electronică sunt folosite în concordanţă cu această politică şi cu legile în vigoare;
- utilizatorii de poştă electronică sunt informaţi asupra modului în care conceptele de securitate şi confidenţialitate se aplică poştei electronice.

Această politică se aplică:

- Sistemului de poştă electronică şi service-ului furnizat de DGP-AMPOPAM
- Tuturor angajaţilor DGP-AMPOPAM
- Tuturor înregistrărilor de poştă electronică ale angajaţilor DGP-AMPOPAM

Această politică se aplică doar poştei electronice în formatul electronic. Această politică nu se aplică copiilor printate ale poştei electronice.

8.4.3.2. Conturile de poştă electronică

Conturile de poştă electronică sunt create de către experţii CIT sau experţii cu atribuţii IT, în concordanţă cu reglementările DGP-AMPOPAM. Fiecare adresă de email are următoarea structură:

prenume.nume@madr.ro

Atunci când o persoană este angajată, directorul direcţiei în care își va desfăşura activitatea trebuie să informeze CIT pentru ca acesta să poată crea un cont de poştă electronică pentru noul angajat.

Atunci când o persoană părăseşte instituţia sau în cazul în care a fost suspendată din cadrul DGP-AMPOPAM, directorul direcţiei în care şi-a desfăşurat activitatea trebuie să informeze CIT. Acesta va şterge căsuţa de poştă electronică.

8.4.3.3. Spaţiul alocat Poştei Electronice

Spaţiul de stocare disponibil pentru stocarea poştei electronice din cadrul DGP-AMPOPAM este limitat de harddisk-ul serverului de poştă electronică. Astfel, utilizatorii de poştă electronică vor avea alocată o anumită parte din spaţiul de stocare pentru primirea de mesaje electronice personale (max. 8 GB). Atunci când această cotă a fost depaşită, utilizatorii trebuie să salveze mesajele electronice pe harddisk-ul local. În acest fel sunt îndepărtate din serverul de mail.

8.4.3.4. Folosirea serviciilor de poştă electronică

Pentru uz personal

Serviciile de poştă electronică pot fi folosite ocazional pentru scopuri personale atâta timp cât nu interferează cu operaţiunile de tehnologie a informaţiei ale DGP-AMPOPAM sau cu serviciile de poştă electronică, nu presupun costuri adiţionale din partea DGP-AMPOPAM sau nu interferează cu munca desfăşurată de angajat.

Restricţii

Serviciile de poştă electronică nu pot fi folosite pentru: activităţi ilegale, scopuri comerciale care nu se află sub auspiciile DGP-AMPOPAM, obţinerea unui câştig financiar sau alte scopuri care contravin politicilor şi liniilor generale stabilite de către DGP-AMPOPAM. Acestea includ, dar nu se limitează, politici în ceea ce priveşte: hărţuire sexuală sau de orice altă natură, activităţi religioase sau politice sau copyright.

Reprezentare

Atunci când trimit un mesaj electronic, utilizatorii serviciilor de poştă electronică trebuie să aibă grijă să nu dea impresia că reprezintă, emit opinii sau fac declaraţii în numele DGP-AMPOPAM sau al oricărui compartiment din cadrul DGP-AMPOPAM cu excepţia cazului în care sunt autorizaţi (în mod implicit sau explicit) să facă acest lucru.

Interferenţa

Serviciile de poştă electronică ale DGP-AMPOPAM nu vor fi folosite pentru scopuri care pot cauza, direct sau indirect, anumite tensiuni excesive asupra reţetelor şi calculatoarelor, sau să interfereze cu folosirea poştei electronice de către ceilalţi. Folosirea include, dar nu se limitează la:

- Transmiterea sau redirecţionarea mesajelor electronice în lanţ;
- "spam", adică, exploatarea serverelor sau a altor sisteme de difuzare pentru unele scopuri care depăşesc scopul iniţial de a amplifica distribuirea pe scară largă a mesajelor electronice nesolicitate; şi
- "Letter-bomb", adică, trimiterea aceluiaşi mesaj electronic către unul sau mai multe destinaţii care interferează cu folosirea normală a poştei electronice.

8.4.3.5. Securitate şi confidenţialitate

Toţi utilizatorii serviciilor de poştă electronică trebuie să ia măsurile necesare pentru a proteja confidenţialitatea mesajelor electronice sau a oricăror înregistrări care conţin informaţii personale şi confidenţiale pe care le-au întâlnit în timpul desfăşurării atribuţiunilor sau în orice alt mod.

În consecinţă, conturile de poştă electronică pot fi accesate doar prin intermediul unei parole. În afara de CIT, doar posesorul contului de email cunoaşte parola respectivă.

Securitatea fizică şi electronică a serverului de poştă electronică este responsabilitatea firmei care asigura accesul la internet, ISP asigurând configurarea, administrarea şi mentenanţa acestuia.

8.4.4. Linii generale pentru construirea parolei şi în ceea ce priveşte sistemul de protecţie

Parolele reprezintă un aspect important în cadrul securităţii computerului. Acestea reprezintă prima linie în protejarea contului de utilizator. O parolă aleasă greşit poate compromite întreaga reţea. Astfel, toţi utilizatorii de calculatoare din cadrul DGP-AMPOPAM sunt responsabili de respectarea paşilor menţionaţi în continuare pentru a găsi şi securiza parolele.

Scopul acestor linii generale este de a stabili un standard pentru creearea unei parole sigure, protejarea acestei parole şi frecvenţa schimbărilor.

Scopul acestei politici este de a include tot personalul care are sau care este responsabili de un cont (sau orice alta formă de acces care necesită sau care suportă o parolă).

Standarde de Construire a Parolei

Parolele sunt folosite în diferite scopuri în cadrul DGP-AMPOPAM inclusiv pentru:

- Accesul la reţea / server aplicatie informatica;
- Folosirea Portal;
- Screen Saver;
- Folosirea aplicaţiilor informatice specifice DGP-AMPOPAM.

Fiecare membru al personalului trebuie să conştientizeze modul în care trebuie alese parolele.

Parolele ineficiente au urmatoarele caracteristici:

- Parola are mai puţin de şase caractere;
- Parola este un cuvânt care poate fi găsit într-un dicţionar (Român, Englez, etc.):
- Parola este un cuvânt comun cum ar fi:
  - Numele de familie, animale preferate, colegi, personaje fantastice;
  - Termeni tehnici şi nume, comenzi, site-uri, companii, aplicaţii software şi hardware;
  - Zile de naştere şi alte informaţii personale cum ar fi adrese şi numere de telefon;
  - Cuvinte şi numere cum ar fi qwerty, zyxwvuts, 12345, 54321, 123321;
  - Oricare din cele menţionate mai sus scrise în ordine inversă;
  - Oricare din cele menţionate mai sus precedate sau urmate de un număr, ex. secret1, 1secret.

Parolele bune au urmatoarele caracteristici:

- Conţin atât majuscule cât şi minuscule;
- Contin numere şi semne de punctuaţie cât şi litere ex., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./;
- Conţin cel putin şase caractere;
- Nu reprezintă un cuvânt în nici o limbă, dialect, jargon, argou;
- Nu se bazează pe informaţii personale, nume de familie;
- Nu sunt niciodată notate sau depozitate on-line.

Toţi utilizatorii trebuie să încerce să creeze parole care pot fi reţinute uşor. O posibilitate ar fi crearea unei parole care are la bază un titlu al unei melodii, afirmaţii sau o altă frază. De exemplu această frază poate fi "Acesta poate fi un mod de a-şi aminti" şi parola poate fi "ApFuMaR!" sau "APFUmar" sau orice alta variaţie. NOTĂ: A nu se folosi nici unul din aceste exemple!

Standarde de Protejare a Parolei

- Nu folosiţi aceeaşi parolă pentru conturile DGP-AMPOPAM şi pentru conturile aferente altei organizaţii e.g. ISP sau cont de mail, servicii bancare online
- Atunci când este cazul, nu folosiţi aceeaşi parolă pentru mai multe căi de acces în DGP-AMPOPAM.
- Toate parolele trebuie să fie considerate drept informaţii confidenţiale:
  - Nu dezvăluiţi parolele DGP-AMPOPAM nimănui, inclusiv asistenţilor administrativi sau secretarelor;
  - Nu dezvăluiţi o parolă prin telefon;
  - Nu dezvăluiţi o parolă într-un mesaj electronic;
  - Nu dezvăluiţi o parolă şefului dumneavoastră;
  - Nu discutaţi despre o parolă în prezenţa altora;
  - Nu oferiţi indicii cu privire la parola dumneavoastră, ex."numele familiei mele";
  - Nu dezvăluiţi o parolă în chestionare şi formulare de securitate;
  - Nu dezvăluiţi o parolă colegilor de birou atunci când plecaţi în vacanţă;
- În cazul în care cineva vă cere să dezvăluiţi parola, faceţi referire la acest document sau rugaţi să contacteze expertul IT;
- Nu folositi aplicaţia "reţineţi parola" ex. Eudora, Outlook, Netscape Messenger etc;
- Nu notaţi parolele şi nu le depozitaţi într-un loc din biroul dumneavoastră. Nu depozitaţi parolele într-un fişier din computerul dumneavostră (inclusiv Notepad, Wordpad, sau alte instrumente similare) fără a fi codate în prealabil;
- În cazul în care o parolă a fost compromisă, acest incident trebuie raportat CIT sau experţilor cu atribuţii IT şi toate parolele vor fi schimbate.

Standarde de dezvoltare a aplicaţiilor

Orice aplicaţie dezvoltată de către DGP-AMPOPAM sau achiziţionată pentru folosinţa personalului DGP-AMPOPAM trebuie să îndeplinească următoarele condiţii:

- Să suporte autentificarea utilizatorilor individuali, nu grupuri;
- Să permită salvarea sau arhivarea periodică a datelor esenţiale ;
- Să nu păstreze parole text sau în orice altă formă uşor de detectat.

8.4.5. Recuperarea datelor în caz de dezastru

În această secţiune se vor face referiri la procedeele de recuperare a datelor în timp scurt şi cu pierderi minime. Atunci când un calculator se defectează, se întrerupe alimentarea cu energie electrică sau intervin alte dezastre, DGP-AMPOPAM trebuie să pună în practică un set de proceduri dinainte stabilite. Este important, deci ca DGP-AMPOPAM să deţină procedurile necesare rezolvării acestor situaţii critice.

Obiectivul principal este de a ajuta DGP-AMPOPAM să supravieţuiască unui dezastru şi să restabilească operaţiunile normale.

Pentru a supravieţui, trebuie să se asigure că operaţiile importante pot reveni la normal în scurt timp. De aceea, DGP-AMPOPAM trebuie să:

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

Obiectele care trebuie recuperate	Surse Potenţiale ale unui Dezastru					Prioritate
	Securitatea Electronică	Eroare Hardware	Foc	Întreruperile de energie	Securitate fizică (Inundaţii/ Furtună/Sabotaj)	
Baza de Date SIMPOP	x	x	x	x	x	1
CD-uri (aplicaţii software din alte organizaţii)	-	-	x	-	x	1
Documentaţia Proiectului	-	-	x	-	x	2
Datele utilizatorului	x	x	x	x	x	1
Servere	x	x	x	x	x	1
Echipament IT			x	x	x	3

Legenda *1 Prioritate Maximă*
5 Prioritate Minimă

Pentru a preveni astfel de situaţii se impune realizarea activităţilor de back-up şi restaurare destinată migrării efectelor situaţiei de urgenţă.

Salvarea Datelor

- Utilizatorii sunt responsabili de propriile date, astfel încât vor realiza back-up-uri periodice peunul din suporturile puse la dispoziție. Datele trebuie stocate pe suporturi sigure. Salvarea datelor media se face folosind ca suport CD, DVD, USB, laptop sau HD extern. Prin achiziția de produse din 2014, DGP-AMPOPAM a asigurat personalului stație de lucru, USB 32 GB, laptop, și HD extern pentru fiecare compartiment, astfel încât să se asigure cel puțin 2 posibilități de salvare a datelor;
- Toate datele trebuie clasificate în funcţie de importanţa în cadrul DGP-AMPOPAM şi salvarea datelor se face în mod corect;
- Mediile de stocare trebuie etichetate cu informaţiile următoare:
  - Salvarea datelor
  - Conţinutul salvării datelor.

- În cazul în care DGP-AMPOPAM a considerat necesară existenţa unui server de partajare a fisierelor, fiecare utilizator poate salva fişiere pe acest server, şi este responsabil de integritatea datelor;
- Procedurile de salvare a datelor trebuie să fie în concordanţă cu prevederile din domeniul informatic referitoare la protejarea datelor critice pentru o organizaţie.

CD-urile cu software şi cele cu backup de date vor fi păstrate într-un spaţiu sigur, un seif sau dulap.

Experţii cu atribuţii IT sunt singurele persoane care au acces la camera sau dulapul în care sunt depozitate CD cu soft sau cu datele salvate.

Se crează copii ale CD-urilor cu software atunci când este necesar.

Restaurarea datelor

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

8.4.6. Managementul userilor în Aplicațiile 2014 gestionate de MFE

Solicitările pentru accesul în aplicațiile gestionate de MFE se vor face conform Procedurii operaționale Activarea unui cont de utilizator al Aplicațiilor 2014 stabilește cadrul general și procedural unitar privind acordarea drepturilor de acces în cadrul Aplicațiilor 2014 gestionate de Ministerul Fondurilor Europene (MySMIS2014, SMIS2014 etc.). Această procedură va fi aplicată de tot personalul DGP-AMPOPAM și OI pentru a putea utiliza aceste aplicații.

Copiile înregistrate ale solicitărilor de acces vor fi transmise experților cu atribuții IT pentru arhivare. Directorul general al DGP-AMPOPAM va direcționa notificările primite de la MFE referitoare la solicitările acces ale personalului DGP-AMPOPAM către experții cu atribuții IT pentru arhivare.

8.4.7. Managementul userilor din cadrul DGP-AMPOPAM în aplicaţia informatică SIMPOP

Mişcările personalului care are acces la resursele informatice vor fi aduse la cunoştinţa expertului IT prin transmiterea de către Directorul General al DGP-AMPOPAM a ordinelor ministrului agriculturii şi dezvoltării rurale / deciziilor directorului general al DGP-AMPOPAM, sau a oricăror documente ce implică accesul în aplicaţia informatică, pentru a crea/bloca conturile, respectiv modificarea drepturilor de acces, de către experţii cu atribuţii IT.

Experţii cu atribuţii IT vor crea/bloca contul utilizatorului în maxim 24 de ore de la primirea informărilor.

În cazul în care ordinul ministrului agriculturii şi dezvoltării rurale se referă la angajarea unui funcţionar public, responsabilul cu gestionarea conturilor, va crea contul de utilizator în sistemul informatic, având drepturile de acces corespunzătoare atribuţiilor compartimentului în care utilizatorul va fi încadrat.

În cazul în care ordinul ministrului agriculturii şi dezvoltării rurale se referă la transferul funcţionarului public în alt compartiment, responsabilul cu gestionarea conturilor va revizui accesul la resursele informatice corespunzător noilor atribuţii de serviciu.

În cazul în care ordinul ministrului agriculturii şi dezvoltării rurale se referă la încetarea raportului de serviciu al funcţionarului, responsabilul cu gestionarea conturilor va bloca imediat toate

conturile de acces la sistemul informatic din cadrul DGP-AMPOP.

În cazul în care decizia directorului general al DGP-AMPOPAM se referă la delegarea unor atribuţii suplimentare unui utilizator, responsabilul cu gestionarea conturilor va revizui accesul la resursele informatice corespunzător noilor atribuţii de serviciu.

Responsabilul cu gestionarea conturilor va ţine o evidenţă strictă a conturilor utilizatorilor.

8.4.8. Managementul userilor aplicaţiei informatice SIMPOP care nu fac parte din personalul DGP-AMPOP

Această activitate se referă la utilizatorii care au acces la sistemul informatic SIMPOP, dar nu fac parte din personalul DGP-AMPOPAM.

În cazul utilizatorilor din cadrul Autorităţii de Certificare, Autorităţii de Audit, Agenţiei de Plată, organismelor intermediare, sau a oricăror structuri cu atribuţii de control naţionale sau europene, responsabilul cu gestionarea conturilor va crea/bloca conturile, respectiv modifica drepturile de acces ca urmare a solicitării scrise a conducătorului structurii respective, aprobată de către directorul general al DGP-AMPOPAM.

În cazul în care este necesar accesul în aplicaţia informatică a unor useri, ca urmare a unui contract de asistenţă tehnică ce are ca beneficiar DGP-AMPOPAM, responsabilul cu gestionarea conturilor va crea/bloca conturile, respectiv modifica drepturile de acces ca urmare a unei decizii a directorului general al DGP-AMPOPAM, ce va cuprinde numele utilizatorilor şi drepturile de acces ce le vor fi atribuite.

9. Responsabilităţi şi răspunderi în derularea activităţii

Nr. crt.	Compartimentul (postul)/acţiunea (operaţiunea)	Director general	Expert IT + CIT (după caz)	furnizori servicii	Tot personalul DGP-AMPOPAM
0	1	2	3	4	5
1	Securitate fizică		E, Ap.		Ap.
2	Securitatea Software		E, Ap.		Ap.
3	Securitatea Comunicaţiilor		E, Ap.		Ap.
4	Securitatea Hardware		E, Ap.		Ap.
5	Securitatea Datelor şi Informaţiilor		E, Ap.		Ap.
6	Administrarea şi menţinerea echipamentelor IT		E, Ap.	E, Ap.	Ap.
7	Media şi Documentaţia		E, Ap.	E, Ap.	Ap.
8	Baza de date		E, Ap.	E, Ap.	Ap.
9	Management resurse umane ce folosesc sistemele informatice	A	Ap.		
10	Activarea unui cont de utilizator al Aplicaţiilor 2014	Aviz			Ap.
11	Arhivare	A	Ap		

E = elaborare; V = verificare; A = aprobare; Ap. = aplicare; Ah. = arhivare

Responsabilităţile expertului IT

Sarcinile şi responsabilităţile experţilor cu atribuţii IT sunt stabilite în Regulamentul de Organizare şi Funcţionare al DGP-AMPOPAM şi prin fişele de post.

Principalele responsabilităţi ale acestora sunt asigurarea mentenanţei şi upgrade-ul periodic al echipamentelor şi sistemelor informatice din cadrul DGP-AMPOPAM, în colaborare cu CIT.

Experţii cu atribuţii IT sunt responsabili, în colaborare cu CIT, de folosirea eficientă a sistemului informaţional şi de căile de comunicare folosite în cadrul DGP-AMPOPAM, cum ar fi poşta electronică, care ajută utilizatorii să îndeplinească sarcinile de serviciu.

10. Lista anexe

Anexele fac parte integrantă din procedura operațională.

Număr anexa	Denumire anexa	Codificare
ANEXA 1	Diagrama reţelei	Formular IT-01
ANEXA 2	Declaraţie de confidenţialitate şi imparţialitate	Formular IT-02

11. Arhivare

Experții cu atribuții IT arhivează, atât în format electronic cât și hârtie:

- copiile înregistrate ale solicitărilor de acces în Aplicațiile 2014 gestionate de MFE, precum și notificările primite de la MFE referitoare la accesul userilor din cadrul DGP-AMPOPAM;

- declarațiile de confidenţialitate şi imparţialitate semnate de personalul DGP-AMPOPAM.

12. Cuprins

ANEXA 1
Formular IT-01

DECLARAŢIE DE CONFIDENŢIALITATE ŞI IMPARŢIALITATE

Subsemnatul(a) ....., având funcţia de ..... la Direcţia Generală Pescuit - Autoritatea de Management pentru POPAM (DGP-AMPOPAM) din cadrul Ministerului Agriculturii şi Dezvoltării Rurale (MADR), declar că îmi voi realiza sarcinile de serviciu în deplină concordanţă cu *Codul de conduită al funcţionarilor public (Legea nr. 7/2004 republicată)*, cu statutul meu de funcţionar public şi în concordanţă cu toate celelalte regulamente aplicabile care guvernează activităţile DGP-AMPOPAM, în toate aspectele care privesc managementul POPAM 2014-2020.

Mă angajez să respect prevederile Codului etic al MADR şi al Planului de securitate informatică al MADR.

Sunt de acord, de asemenea, să păstrez confidenţialitatea asupra informaţiilor sau documentelor (dacă sunt considerate confidenţiale, privilegiate, private, personale sau altele) încredinţate sau descoperite de mine în cursul sau ca rezultat al participării mele la activităţile DGP-AMPOPAM şi înţeleg ca aceste informaţii să nu le dezvălui vreunei terţe părţi.

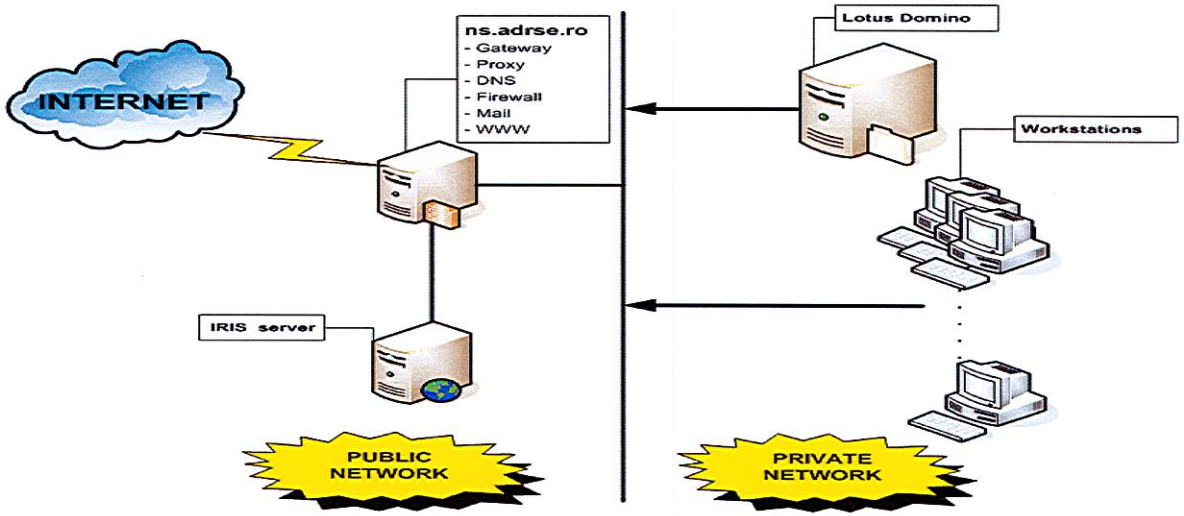
Mai mult, declar că voi păstra secretul profesional pe durata angajării mele în cadrul DGP-AMPOPAM, şi nu voi comunica nici unei persoane sau entităţi vreo informaţie încredinţată mie sau descoperită de mine, sau să fac publică orice informaţie, şi nu voi utiliza, în mod prejudicios, orice informaţie furnizată mie.

Nume şi prenume .....
Semnătura .....
Data .....

ANEXA 2

Formular IT-02

Diagrama Reţelei



Structura DGP-AMPOPAM

Există aproximativ 110 staţii de lucru conectate în Reţeaua Locală. Sisteme de operare sunt Windows, diferite versiuni. Toate serverele se găsesc într-o singură cameră. DGP-AMPOPAM este conectată la internet prin intermediul Serviciului de Telecomunicaţii Speciale. Infrastructura logică a DGP-AMPOPAM este prezentată în Diagrama Reţelei prezentată mai sus.