

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

MINISTERUL ADMINISTRAȚIEI ȘI INTERNELOR
Nr. 279 din 17 decembrie 2012

MINISTERUL FINANTELOR PUBLICE
Nr. 1.736 din 20 decembrie 2012

ORDIN

privind aprobarea modelului-cadru al protocolului de cooperare în vederea schimbului de informații între Agenția Națională de Administrare Fiscală și autoritățile administrației publice locale

Având în vedere prevederile art. 11 alin. (32) și art. 228 alin. (22) și (3) din Ordonanța Guvernului nr. 92/2003 privind Codul de procedură fiscală, republicată, cu modificările și completările ulterioare, și ale art. 19 din anexa nr. 1 la Hotărârea Guvernului nr. 717/2009 privind aprobarea normelor de implementare a programului „Prima casă”, cu modificările și completările ulterioare,

în temeiul prevederilor art. 7 alin. (5) și (7) din Ordonanța de urgență a Guvernului nr. 30/2007 privind organizarea și funcționarea Ministerului Administrației și Internelor, aprobată cu modificări prin Legea nr. 15/2008, cu modificările și completările ulterioare, și ale art. 10 alin. (4) din Hotărârea Guvernului nr. 34/2009 privind organizarea și funcționarea Ministerului Finanțelor Publice, cu modificările și completările ulterioare,

ministrul administrației și internelor și viceprim-ministrul, ministrul finanțelor publice, emit următorul ordin:

Art. 1. — Pentru realizarea schimbului de informații între Agenția Națională de Administrare Fiscală și autoritățile administrației publice locale se aprobă modelul-cadru al protocolului de cooperare, conform anexei care face parte integrantă din prezentul ordin.

Art. 2. — (1) Prelucrările de date cu caracter personal efectuate potrivit scopului prevăzut la art. 1 se fac cu respectarea dispozițiilor Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter

personal și liberă circulație a acestor date, cu modificările și completările ulterioare.

(2) În accepțiunea art. 3 lit. e) din Legea nr. 677/2001, cu modificările și completările ulterioare, Agenția Națională de Administrare Fiscală este operator de date cu caracter personal pentru prelucrările efectuate în baza de date care face obiectul protocolului prevăzut la art. 1.

Art. 3. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

p. Ministrul administrației și internelor,
Ion Stoica,
secretar general

Viceprim-ministru, ministrul finanțelor publice,
Florin Georgescu

Contrasemnează:
Ministrul delegat pentru administrație,
Radu Stroe

ANEXĂ

AGENȚIA NAȚIONALĂ DE ADMINISTRARE FISCALĂ
Nr. / 20...

UNITATEA/SUBDIVIZIUNEA ADMINISTRATIV-TERITORIALĂ
Nr. / 20...

PROTOCOL DE COOPERARE

În temeiul următoarelor prevederi legale:

- Legea administrației publice locale nr. 215/2001, republicată, cu modificările și completările ulterioare;
- Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și liberă circulație a acestor date, cu modificările și completările ulterioare;
- art. 11, 61 și 62 din Ordonanța Guvernului nr. 92/2003 privind Codul de procedură fiscală, republicată, cu modificările și completările ulterioare;
- art. 5 alin. (1) lit. g) din Hotărârea Guvernului nr. 109/2009 privind organizarea și funcționarea Agenției Naționale de Administrare Fiscală, cu modificările și completările ulterioare;
- Hotărârea Guvernului nr. 717/2009 privind aprobarea normelor de implementare a programului „Prima casă”, cu modificările și completările ulterioare;
- Ordinul ministrului finanțelor publice nr. 2.875/2009 pentru aprobarea instrucțiunilor privind utilizarea sistemului informatic din cadrul Ministerului Finanțelor Publice*);
- Ordinul ministrului finanțelor publice nr. 551/2003 pentru aprobarea Instrucțiunilor de aplicare a prevederilor titlului I — „Transparența informațiilor referitoare la obligațiile bugetare restante” al cărții I din 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, privind transparența administrației publice centrale și locale și parteneriat cu cetățenii;

*) Ordinul ministrului finanțelor publice nr. 2.875/2009 pentru aprobarea instrucțiunilor privind utilizarea sistemului informatic din cadrul Ministerului Finanțelor Publice nu a fost publicat în Monitorul Oficial al României, Partea I.

— Legea nr. 455/2001 privind semnătura electronică;
 — Hotărârea Guvernului nr. 1.259/2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, cu modificările ulterioare,
 Ministerul Finanțelor Publice, prin Agenția Națională de Administrare Fiscală, denumită în continuare ANAF, cu sediul în București, str. Apolodor nr. 17, sectorul 5, reprezentată prin domnul, în calitate de președinte,
 și
 Unitatea/subdiviziunea administrativ-teritorială, cu sediul în, reprezentată prin domnul, în calitate de,
 denumite în continuare *părți*, au convenit la încheierea prezentului protocol.

ARTICOLUL 1

Obiectul protocolului

Obiectul protocolului îl reprezintă cooperarea între instituții publice, prin schimbul de informații în formă dematerializată, în scopul:

- a) creșterii nivelului de colectare a taxelor și impozitelor la bugetul general consolidat al statului;
- b) prevenirii și combaterii evaziunii fiscale;
- c) facilitării accesului persoanelor fizice și juridice la informații deținute de instituțiile publice semnate.

ARTICOLUL 2

Obligațiile părților

În termen de maximum 30 de zile de la data semnării prezentului protocol părțile vor stabili și vor semna procedura de lucru comună. Procedura de lucru se va semna la nivelul structurilor tehnice ale celor două instituții și va conține toate detaliile privind modalitatea de implementare a serviciilor din punct de vedere organizatoric și procedural.

În îndeplinirea obiectivelor prezentului protocol, cele două părți semnate au obligația respectării prevederilor referitoare la protejarea secretului fiscal din Ordonanța Guvernului nr. 92/2003 privind Codul de procedură fiscală, republicată, cu modificările și completările ulterioare.

2.1. Obligațiile unității/subdiviziunii administrativ-teritoriale

2.1.1. Unitatea/Subdiviziunea administrativ-teritorială va asigura accesul la informații, în formă dematerializată, personalului ANAF desemnat în acest scop, conform anexei nr. 1, privind:

- a) patrimoniul persoanelor fizice și juridice (bunuri imobile și bunuri mobile) și rolul nominal unic;
- b) creanțele datorate de contribuabili (persoane fizice și juridice) bugetului general al unității/subdiviziunii administrativ-teritoriale.

2.1.2. Unitatea/Subdiviziunea administrativ-teritorială:

a) va respecta prevederile legale referitoare la protecția datelor personale și a informațiilor fiscale, prin utilizarea informațiilor din bazele de date ale Ministerului Finanțelor Publice numai în scopurile prevăzute de lege;

b) va solicita certificat digital pentru personalul desemnat al unității/subdiviziunii administrativ-teritoriale pentru accesarea serviciilor oferite de sistemul informatic al Ministerului Finanțelor Publice;

c) va respecta procedura și normele de conectare la rețea și la serviciile oferite de sistemul informatic al Ministerului Finanțelor Publice, stabilite de către Ministerul Finanțelor Publice și Serviciul de Telecomunicații Speciale;

d) va solicita la ANAF înrolarea certificatelor digitale obținute pentru funcționari în sistemul de management al identității și rolurilor utilizatorilor sistemului informatic al Ministerului Finanțelor Publice, folosind tabelul din anexa nr. 2. Datele din anexa nr. 2 vor fi centralizate în format electronic de către unitățile/subdiviziunile administrativ-teritoriale și trimise către Direcția generală a tehnologiei informației din cadrul Ministerului Finanțelor Publice, în format electronic. În cazul în care informațiile ce țin de furnizarea serviciilor, transmise de unitățile/subdiviziunile administrativ-teritoriale, sunt eronate, Ministerul Finanțelor Publice nu are nicio responsabilitate privind întârzierile în activarea/dezactivarea rolurilor;

e) va solicita modificări în ceea ce privește identitatea și rolurile pe care le dețin persoanele titulare de certificate digitale imediat ce acestea sunt necesare, anunțând Direcția generală a tehnologiei informației din cadrul Ministerului Finanțelor Publice, în vederea modificării/revocării prin formularul din anexa nr. 3;

f) va asigura cunoașterea și respectarea de către personalul desemnat al unității/subdiviziunii administrativ-teritoriale a prevederilor anexei la Ordinul ministrului finanțelor publice nr. 2.875/2009, respectiv anexa nr. 4, inclusiv însușirea și respectarea prevederile referitoare la utilizarea suporturilor (externe) de certificate digitale;

g) va lista și păstra registrul de evidență al accesului, generat automat de serviciul oferit de sistemul informatic al Ministerului Finanțelor Publice;

h) va colabora cu Serviciul de Telecomunicații Speciale în vederea asigurării accesului securizat al personalului desemnat al unităților/subdiviziunilor administrativ-teritoriale la sistemul informatic al Ministerului Finanțelor Publice.

2.2. Obligațiile ANAF

2.2.1. ANAF va respecta prevederile legale referitoare la protecția datelor personale și a informațiilor fiscale, prin utilizarea informațiilor din bazele de date ale unității/subdiviziunii administrativ-teritoriale numai în scopurile prevăzute de lege.

2.2.2. ANAF va asigura accesul la informații, în formă dematerializată, personalului unității/subdiviziunii administrativ-teritoriale desemnat în acest scop, în cadrul serviciului oferit de sistemul informatic al Ministerului Finanțelor Publice, la următoarele informații referitoare la:

- a) deținerea de conturi bancare;
- b) obligațiile de plată a contribuțiilor sociale, impozitului pe venit și evidența nominală a persoanelor asigurate care au domiciliul fiscal pe raza teritorială a unității/subdiviziunii administrativ-teritoriale;
- c) veniturile din salarii și aferente salariilor, precum și cele din venituri din alte surse obținute de contribuabili persoane fizice care au domiciliul fiscal pe raza teritorială a unității/subdiviziunii administrativ-teritoriale, denumirea și codul unic de identificare a angajatorului.

2.2.3. Direcția generală a tehnologiei informației din cadrul Ministerului Finanțelor Publice:

a) va înrola în sistemul de management al identității și rolurilor al Ministerului Finanțelor Publice, în baza solicitărilor făcute de unitatea/subdiviziunea administrativ-teritorială, certificatele digitale și va acorda drepturi de acces personalului desemnat al unității/subdiviziunii administrativ-teritoriale, în temeiul acestor solicitări;

b) va modifica drepturile de acces ale personalului desemnat de unitatea/subdiviziunea administrativ-teritorială în baza solicitărilor făcute de aceasta în sistemul de management al identității și rolurilor al Ministerului Finanțelor Publice;

c) va asigura personalului unității/subdiviziunii administrativ-teritoriale instruirea și asistența tehnică necesară operării în serviciile oferite de sistemul informatic al Ministerului Finanțelor Publice, conform procedurilor Ministerului Finanțelor Publice de instruire a personalului și de soluționare a incidentelor în sistemul informatic;

d) va colabora cu Serviciul de Telecomunicații Speciale în vederea asigurării accesului securizat al personalului desemnat

al unităților/subdiviziunilor administrativ-teritoriale la sistemul informatic al Ministerului Finanțelor Publice.

ARTICOLUL 3

Modalități de realizare a schimbului de informații

3.1. Schimbul de informații între părți (actualizarea bazelor de date) se va realiza periodic, cu respectarea legislației în vigoare, conform procedurii de lucru comune.

3.2. Schimbul de informații stabilit prin acest protocol se va realiza prin mecanisme securizate, cu drept de citire pentru ambele părți.

3.3. Formatul datelor transmise și periodicitatea actualizării se stabilesc de comun acord prin procedura de lucru comună.

ARTICOLUL 4

Dispoziții finale

4.1. Datele și informațiile furnizate de părți sunt confidențiale și se utilizează și se păstrează conform prevederilor legale și normelor interne în vigoare.

Prezentul protocol s-a încheiat în două exemplare originale, câte unul pentru fiecare parte.

AGENȚIA NAȚIONALĂ DE ADMINISTRARE FISCALĂ

UNITATEA ADMINISTRATIV-TERITORIALĂ/
SUBDIVIZIUNEA ADMINISTRATIV-TERITORIALĂ

Președinte,

Reprezentant,

ANEXA Nr. 1
la protocol

AGENȚIA NAȚIONALĂ DE
ADMINISTRARE FISCALĂ

Solicitare actualizare utilizatori servicii oferite de sistemul informatic al Primăriei

Prin prezenta, vă solicităm dreptul de acces pentru funcționarii Agenției Naționale de Administrare Fiscală la serviciile oferite de sistemul informatic al Primăriei

Numele	Prenumele	Codul numeric personal	E-mail	Telefon	Componenta aplicație	Tipul operației

LEGENDA

Tipul operației: consultare

Componenta aplicație: IMPOZITE ȘI TAXE LOCALE

Tipul accesului la sistemul informatic al primăriei, prin rețea securizată de STS..... (alte situații)

Agencia Națională de Administrare Fiscală

Președinte

(numele, prenumele și semnătura)

Data

.....

Solicitățile de useri, pentru evidența utilizatorilor, se trimit la adresa de e-mail a Primăriei

ANEXA Nr. 2
la protocol

Instituția

Solicitare actualizare utilizatori servicii oferite de sistemul informatic al Ministerului Finanțelor Publice

Prin prezenta vă solicităm dreptul de acces pentru funcționarii primăriei noastre la serviciile oferite de sistemul informatic al Ministerului Finanțelor Publice.

Numele	Prenumele	Codul numeric personal	E-mail	Telefon	Componenta aplicație	Tipul operației

LEGENDA

Tipul operației: consultare

Componenta aplicație: ASIGSOC; ASIGSOC/BĂNCI; PATRIMONIU; TRASABILITATE

Tipul accesului la sistemul informatic al Ministerului Finanțelor Publice, prin rețea securizată de STS (alte situații)

Data

.....

 Primar al,
(numele, prenumele și semnătura)

Solicitările de utilizatori, pentru evidența utilizatorilor, se trimit la adresa de e-mail help.extranet@mfinante.ro

ANEXA Nr. 3
la protocol

Instituția

Modificare/Ștergere drepturi utilizatori servicii oferite de sistemul informatic al Ministerului Finanțelor Publice

Tipul operației	Componenta aplicație	Numele	Prenumele	Județul	Tipul structurii	Numele unității	Numele unității (denumirea scurtă)	Codul numeric personal	ID-ul utilizatorului	Seria certificatului digital	E-mail	Telefon

LEGENDĂ

Tipul operației: modificare; ștergere

Componenta aplicație: ASIGSOC; ASIGSOC/BĂNCI; PATRIMONIU; TRASABILITATE

Tipul structurii: felul primăriei, cu rețea securizată sau fără

Județul: pentru central, municipiul București

Solicitările de utilizatori, pentru evidența utilizatorilor, se trimit la adresa de e-mail help.extranet@mfinante.ro

Anexa la Ordinul ministrului finanțelor publice nr. 2.875/13.10.2009*)

INSTRUCȚIUNI

privind utilizarea sistemului informatic din cadrul Ministerului Finanțelor Publice

CAPITOLUL I

Dispoziții generale

Art. 1. — Prezentele instrucțiuni sunt elaborate în scopul asigurării securității informațiilor în format electronic din cadrul Ministerului Finanțelor Publice, denumit în continuare *MFP*, și stabilesc reguli privind protejarea sistemului informatic al ministerului, conform legislației române în vigoare, precum și convențiilor internaționale și reglementărilor comunitare semnate de România sau în care România este parte (în acest sens Standardul ISO/IEC 1779 adus la zi la ISO/IEC 27002:2005 fiind considerat ca principal ghid pentru domeniul securității informaționale).

Art. 2. — În sensul prezentelor instrucțiuni, termenii de mai jos au următoarele definiții:

a) *administrator de rețea* — persoană calificată în domeniul tehnologiei informației, desemnată să gestioneze utilizatorii finali, resursele hardware și software și modul de acces la resursele rețelei de date;

b) *blocare acces stație de lucru* — set de comenzi specific stației de lucru care permite interzicerea imediată a accesului de la tastatură la stația de lucru;

c) *dispozitiv wireless* — echipament de tehnică de calcul și comunicații care poate asigura conectarea la rețele de comunicații prin unde radio;

d) *echipamente periferice* — imprimantele, scanerele, multifuncționalele, unitățile mobile disc flexibil, unitățile mobile hard disk, modemurile;

e) *fișier multimedia* — fișier având o organizare internă dedicată stocării unei combinații de formate text, audio, fotografie, animație, film și conținut interactiv;

f) *medii/suporturi externe de stocare a datelor* — bandă magnetică, disc fix, dischetă, casetă, CD-ROM/RW, DVD-ROM/RW, chei USB flash/stick, HDD extern portabil;

g) *nume de utilizator (user name)* — cod alfanumeric atribuit persoanei care urmează să acceseze resurse ale sistemului informatic;

h) *parola de acces (password)* — cod (șir de caractere) primit odată cu stația/aplicația, folosit pentru accesarea resurselor. Parola trebuie schimbată de utilizator de la prima folosire, astfel încât să nu fie cunoscută decât de acesta;

i) *patch cord* — cablul de rețea care face legătura între stație și priza de rețea montată pe perete;

j) *proprietar al drepturilor asupra informațiilor* — persoana angajată sau numită într-o funcție publică în cadrul MFP care are responsabilitatea stabilirii și urmăririi regulilor de utilizare și gestionare a datelor stocate sau prelucrate printr-un serviciu informatic, precum și de stabilire a condițiilor de schimb de informații cu alte organizații;

k) *resursele sistemului informatic* — echipamentele de tehnologia informației (serve, stații de lucru, imprimante, scanere etc.), rețelele de comunicații de date LAN, MAN, WAN, alte componente și instalații (climatizare, alimentare cu energie, stingere incendiu, control acces fizic etc.), mediile de stocare a datelor, software-ul de bază, aplicațiile informatice, programele utilitare, datele, bazele de date, fișierele, sistemele de protecție

a datelor, personalul ce exploatează și întreține resursele sistemului informatic, documentațiile de proiectare, documentațiile de exploatare etc., procedurile de lucru, planurile de continuitate, teoriile ce stau la baza algoritmilor de prelucrare etc.;

l) *responsabil cu alimentarea electrică* — Direcția generală de investiții, achiziții publice și servicii interne și compartimentele din instituțiile publice subordonate aflate în coordonarea sa metodologică;

m) *responsabil cu întreținerea echipamentelor TIC* — Direcția generală a tehnologiei informației, denumită în continuare *DGTI*, și compartimentele din instituțiile publice subordonate aflate în coordonarea sa metodologică;

n) *rețea de date/rețea de comunicații de date* — subsansamblu al sistemului informatic format din patch corduri, prize de rețea, cablaj structurat, echipamente de comunicații, protocoale de comunicații și software pentru administrarea comunicațiilor. Rețeaua de date are rolul de a oferi suport hardware și software pentru interconectarea stațiilor de lucru, serverelor, imprimantelor etc. și pentru acces la serviciile informatice, inclusiv la poșta electronică și internet;

o) *serviciu informatic* — unul sau mai multe subsisteme ale sistemului informatic care permit desfășurarea unui proces de lucru în cadrul organizației;

p) *sistemul de management al identității <MgmtId>* — sistem centralizat de autentificare a utilizatorilor și management al drepturilor de acces ale utilizatorilor la resursele sistemului informatic;

q) *sistem informatic* — ansamblul de elemente care asigură introducerea, prelucrarea, stocarea, transmiterea și extragerea datelor pe cale electronică realizat în scopul oferirii de servicii informatice;

r) *stație de lucru* — ansamblul format din calculator și echipamentele periferice destinat realizării sarcinilor de serviciu, conectat sau nu la rețeaua de date a MFP și care are sau nu acces la alte resurse ale sistemului informatic;

s) *stație de lucru mobilă/stație mobilă* — laptop, tabletă electronică, asistent personal electronic (PDA), agendă electronică, telefon mobil inteligent;

t) *UPS* — sursă neîntreruptibilă de tensiune; asigură alimentarea cu energie electrică a consumatorilor, un timp limitat, în cazul lipsei tensiunii în rețeaua publică;

u) *utilizatorul final/responsabilul stației de lucru* — persoana angajată sau numită într-o funcție publică în cadrul MFP, care a primit dreptul de acces la stația de lucru și drepturi de utilizare a resurselor sistemului informatic.

CAPITOLUL II

Reguli de utilizare a stației de lucru

SECȚIUNEA 1

Întreținerea și urmărirea stării de funcționare a stației de lucru

Art. 3. — Stația de lucru se utilizează în conformitate cu instrucțiunile specifice primite de responsabilul stației de lucru odată cu echipamentul.

*) Ordinul ministrului finanțelor publice nr. 2.875/2009 pentru aprobarea instrucțiunilor privind utilizarea sistemului informatic din cadrul Ministerului Finanțelor Publice nu a fost publicat în Monitorul Oficial al României, Partea I.

Art. 4. — Pentru a asigura buna funcționare a stației, responsabilul stației de lucru are următoarele îndatoriri:

a) să verifice că în exterior, pe carcasa stației de lucru, sunt marcate numele instituției și numărul de inventar și să păstreze copia fișei de inventar a stației de lucru, precum și a celorlalte echipamente de calcul aflate în inventarul său;

b) să amplaseze stația astfel încât să poată fi utilizată cu ușurință și totodată ferită de lovirea accidentală, de șocuri și vibrații, ferită de acțiunea directă a razelor solare, ferită de praf, fum, ploaie și umezeală;

c) să pozeze cablurile astfel încât să nu împiedice circulația personalului;

d) să poziționeze stația în așa fel încât cablurile să fie protejate;

e) să se asigure că alimentarea stației de lucru se face din prizele de alimentare special destinate pentru aceasta sau din UPS;

f) să nu folosească, pe cât posibil, pentru alimentarea stației de lucru prelungitoare;

g) dacă este necesară folosirea unui prelungitor, acesta trebuie să suporte curentul absorbit de stație;

h) să verifice zilnic starea prizelor electrice, a cablurilor de alimentare și a prelungitoarelor (dacă apar deformare mecanică, încălzire excesivă sau alte asemenea probleme care pot periclita alimentarea în parametri nominali cu energie electrică a stației de lucru ori reprezintă pericol de incendiu sau electrocutare);

i) să nu folosească prizele și prelungitoarele de alimentare pentru stația de lucru la alimentarea altor consumatori: aparate de aer condiționat, fierbătoare, frigider, aspiratoare etc.;

j) să deconecteze stația de lucru de la prizele de alimentare în cazul în care cordonul de alimentare s-a deteriorat, în echipament s-a scurs lichid, echipamentul a fost expus la apă sau la ploaie, din echipament iese fum;

k) să deconecteze stația de lucru de la prizele de alimentare în cazul în care nu este folosită o perioadă mai îndelungată: sfârșit de săptămână, sărbători, concediu etc.;

l) să verifice că patch cordul nu trece pe lângă cabluri de alimentare electrică, surse de căldură și că nu intersectează locuri de trecere pentru personal;

m) dacă există echipamente periferice, să le urmărească funcționarea și să cunoască semnalele de avertizare în caz de funcționare incorectă a acestora;

n) dacă există unități disc flexibil, CD sau DVD, să utilizeze discuri curate, fără urme de deteriorare mecanică, să utilizeze butoanele de deschidere a unității disc flexibil, CD sau DVD și să nu forțeze suportul disc flexibil, CD, DVD prin împingere sau tragere;

o) să sesizeze de urgență defectele observate, în funcție de specificul defecțiunii, responsabilului cu alimentarea electrică sau punctului de contact Help desk;

p) să nu deterioreze sigiliul stației de lucru, să nu deterioreze sau să nu distrugă etichetele aplicate pe echipamente;

q) să sprijine personalul abilitat pentru remedierea defecțiunilor, furnizând informații privind anomaliile de funcționare observate;

r) să folosească medii/suporturi externe de stocare a datelor numai dacă are permisiunea și programul antivirus este activ și actualizat la zi.

Art. 5. — Responsabilul stației de lucru trebuie să protejeze stația de lucru, următoarele activități fiind interzise:

a) să realizeze conexiuni între echipamentele de calcul, altele decât cele realizate de administratorul de rețea și responsabilul cu întreținerea echipamentelor TIC;

b) să schimbe prizele de rețea;

c) să schimbe echipamentele periferice;

d) să înlocuiască monitorul, mouse-ul sau tastatura;

e) să aproprie stația de surse de încălzire la o distanță mai mică de 1 m;

f) să obtureze sistemul de ventilație al stației de lucru;

g) să mențină stația în funcțiune la temperaturi ale mediului ambiant mai mari de 35 grade Celsius;

h) să utilizeze în apropierea stației substanțe chimice corozive, toxice sau inflamabile;

i) să utilizeze stația cu mâinile ude sau murdare;

j) să lovească stația sau să o supună șocurilor ori vibrațiilor;

k) să depoziteze obiecte pe echipamente ori pe cabluri;

l) să mănânce, să bea la o distanță mai mică de 1 m de stație sau să fumeze în încăperea în care se află stația.

SECȚIUNEA a 2-a

Politica de utilizare a informațiilor din MFP

Art. 6. — Informațiile stocate în sistemul informatic, precum și informațiile privind sistemul informatic și resursele acestuia, inclusiv configurarea, organizarea, dezvoltarea și exploatarea sa, sunt proprietatea MFP, utilizatorul neavând dreptul de a pretinde asigurarea confidențialității sau intimității sub pretextul caracterului personal al datelor.

Art. 7. — Resursele informatice ale MFP se vor utiliza numai în scopul îndeplinirii sarcinilor de serviciu.

Art. 8. — Toate informațiile din sistemul informatic al MFP pot fi interceptate, monitorizate, controlate, analizate și arhivate de administratorii de rețea numai în conformitate cu sarcinile de serviciu.

Art. 9. — Lucrările cu caracter personal se pot efectua folosind resursele MFP numai cu acordul conducerii direcției în care utilizatorul își desfășoară activitatea.

Art. 10. — Nu se vor stoca sau prelucra în sistemul informatic al MFP informații care nu au legătură cu sarcinile de serviciu.

Art. 11. — Utilizatorii sunt obligați să respecte măsurile prevăzute în anexa nr. 1 „Securitatea sistemelor informatice și a comunicațiilor de date”.

SECȚIUNEA a 3-a

Accesul la serviciile stației de lucru și ale sistemului informatic

Art. 12. — Dreptul de acces la stație și/sau la sistemul informatic îl are numai persoana nominalizată drept utilizator final.

Art. 13. — Administratorii de rețea au acces la stația de lucru a unui utilizator ca urmare a solicitării utilizatorului sau cu ocazia desfășurării activității de mentenanță ori în alte situații aprobate de conducerea MFP sau a direcției, după caz.

Art. 14. — Drepturile de acces la informațiile de pe serverele din rețea se vor acorda de către DGTI conform regulilor stabilite de proprietarul drepturilor asupra informațiilor, în baza unei cereri scrise a conducătorului direcției solicitantului și aprobate de proprietarul drepturilor asupra informațiilor.

Art. 15. — Proprietarul drepturilor asupra informațiilor stabilește scopul și drepturile de utilizare a informațiilor și serviciilor informatice, precum și regulile de protejare și manipulare a informațiilor.

Art. 16. — Proprietarul drepturilor asupra informațiilor stabilește împreună cu DGTI controale adecvate pentru a detecta eventuale încălcări ale regulilor de protejare și manipulare a informațiilor.

Art. 17. — Utilizatorilor le este interzis să acceseze date la care nu au drept de acces.

Art. 18. — Accesul la stație se va face utilizând un nume de utilizator (user name) și o parolă de acces (password), care vor fi cunoscute numai de responsabilul stației.

Art. 19. — Responsabilul stației nu trebuie să permită accesul altor utilizatori la stația de care răspunde.

Art. 20. — Drepturile de acces la nivel de stație vor fi permise utilizatorului numai de tip limitat, nu și drepturi de administrare.

Art. 21. — Accesul de tip „administrator” la nivel de stație se va face numai de către administratorul de rețea autorizat, care trebuie să cunoască parola adecvată.

Art. 22. — Utilizatorii sunt obligați să respecte Procedura pentru asigurarea accesului autorizat la stațiile de lucru și la aplicațiile informatice centralizate în intranetul Ministerului Finanțelor Publice, prevăzută în anexa nr. 2.

Art. 23. — În rețeaua de date a MFP pot fi conectate numai echipamentele proprietatea MFP, configurate de administratorul de rețea.

Art. 24. — Este interzisă conectarea în rețeaua de date a MFP de echipamente care nu sunt proprietatea MFP (de exemplu: dispozitive wireless de conectare directă la internet).

Art. 25. — Este interzisă conectarea în rețeaua de date a MFP de echipamente care nu au fost configurate de administratorul de rețea.

SECȚIUNEA a 4-a

Parola de acces

Art. 26. — Parola de acces este proprietatea personală a utilizatorului final, care va fi obligat să respecte următoarele reguli:

a) nu va afișa parola de acces prin scriere/tipărire pe hârtie sau post-it sau alte asemenea suporturi;

b) nu va transmite parola de acces altor persoane, inclusiv colegilor de birou, chiar dacă aceștia se oferă să îi ajute în utilizarea stației de lucru;

c) înainte de plecarea din sediu pentru perioade mai mari de timp (delegații, concedii etc.) va pune la dispoziția colegilor săi datele care le-ar putea fi necesare pentru buna desfășurare a activității, astfel încât aceștia să nu aibă nevoie ulterior de parola sa de acces;

d) dacă trebuie să lucreze pe o altă stație decât cea pentru care este responsabil, el va folosi propriul nume de utilizator (user name) și parola de acces (password) proprie pentru a accesa această stație, dacă aceasta este într-un domeniu; în caz contrar, administratorul de rețea va crea un nou cont pentru acel utilizator;

e) nu va încerca să anuleze parolele de acces pentru BIOS, dacă acestea există;

f) asigură protejarea accesului la date prin blocarea stației de lucru ori de câte ori este obligat să se deplaseze de lângă aceasta;

g) este singurul răspunzător de confidențialitatea parolei de acces, aceasta fiind mijlocul de autentificare și prima barieră în cazul unei tentative de acces neautorizat la resurse.

SECȚIUNEA a 5-a

Securitatea și protecția software-ului și a informațiilor de pe stația de lucru

Art. 27. — Utilizatorul trebuie să cunoască modul de operare/utilizare, pornire/oprire a stației de lucru, precum și modul de utilizare a aplicațiilor necesare desfășurării activităților curente din cadrul direcției în care activează.

Art. 28. — Instalarea oricărui program pe stațiile de lucru și serverele MFP se efectuează numai de către personalul autorizat al DGTI. Utilizatorul final nu are dreptul să instaleze nicio/niciun aplicație, utilitar, program sau alt tip de software și nici să actualizeze versiuni ale acestora.

Art. 29. — Întreținerea, refacerea, reinstalarea, depanarea software sau/și hardware în vederea funcționării corecte a sistemului de operare și a aplicațiilor se vor face numai de către persoanele autorizate în acest sens, respectiv de către personalul DGTI.

Art. 30. — În cazul în care este necesară instalarea unui produs software pentru evaluare, testare sau pentru îndeplinirea sarcinilor de serviciu, utilizatorul se va adresa DGTI printr-o cerere avizată de către superiorul ierarhic, prezentând sarcina de serviciu care motivează această necesitate.

Art. 31. — Este interzisă rularea pe echipamentele de calcul și telecomunicații ale MFP a oricărei/oricărui aplicații, utilitar, program sau alt tip de software dobândit în nume propriu.

Art. 32. — Introducerea prin instalare, compilare, copiere, descărcare de cod neautorizat pe componentele sistemului informatic al MFP este interzisă. Numai programele care beneficiază de o licență validă și aprobate de MFP pot fi instalate pe echipamentele de calcul și telecomunicații ale MFP. Această regulă se aplică inclusiv descărcării de programe de pe serviciile publice.

Art. 33. — Detectarea programelor neautorizate sau modificărilor neautorizate ale programelor ori ale parametrilor sistemelor poate face obiectul unei investigații oficiale.

Art. 34. — Pentru protecția împotriva atacurilor informatice este necesară activarea aplicației de tip firewall de pe stațiile de lucru.

Art. 35. — În cazul suspiciunii de infectare informatică, utilizatorul final nu are dreptul să acționeze din proprie inițiativă. El trebuie să oprească utilizarea echipamentului în cauză, să îl lase în starea în care acesta se găsește și să informeze punctul de contact Help desk al DGTI. Deparazitarea/Ștergerea fișierelor infectate detectate se va realiza de personalul de specialitate al DGTI.

Art. 36. — Utilizatorul nu are voie să oprească sau să dezinstaleze programul de protecție antivirus și nici să instaleze alte programe antivirus. Orice modificare se va face numai cu acceptul DGTI.

Art. 37. — Nu se vor utiliza medii/suporturi externe de stocare a datelor pentru introducerea/salvarea de date și nu se vor salva fișiere din internet dacă programul de protecție antivirus este oprit.

Art. 38. — În cazul în care folosește programe fără înștiințarea și aprobarea DGTI, utilizatorul este direct răspunzător de efectele produse de încălcarea Legii nr. 8/1996 privind dreptul de autor și drepturile conexe, cu modificările și completările ulterioare.

Art. 39. — Numai proprietarul drepturilor asupra informațiilor poate autoriza ieșirea datelor din birou sau din sediu ori transmiterea datelor în afara organizației.

Art. 40. — Înainte de predarea definitivă a stației de lucru, responsabilul acesteia este obligat să salveze toate datele utile pe medii/suporturi externe de stocare a datelor și apoi să șteargă toate informațiile de pe stația de lucru care urmează a fi predată.

Art. 41. — Înainte de părăsirea definitivă a postului, utilizatorul este obligat să predea toate mediile/suporturile externe de stocare a datelor pe care s-au efectuat salvări de informații utile șefului său ierarhic.

Art. 42. — În scopul prevenirii eventualelor neglijențe sau a acțiunilor răuvoitoare, în cazul reutilizării stațiilor de lucru sau în cazul casării acestora, serviciul sau direcția proprietară a datelor va comunica DGTI gradul de confidențialitate al informațiilor stocate, hotărând, după caz:

a) distrugerea fizică organizată: distrugerea controlată a hard-diskurilor, a suporturilor de stocare de date;

b) autorizarea reutilizării stațiilor de lucru după un control prealabil: ștergerea sigură a configurațiilor, ștergerea sigură a datelor prin rescrierea repetată a suportului.

CAPITOLUL III

Alte dispoziții

SECȚIUNEA 1

Reguli pentru stocarea și transportul suporturilor externe de stocare a datelor

Art. 43. — Suporturile externe de stocare a datelor se inscripționează de utilizatorul stației de lucru cu numele instituției și al compartimentului (direcției) care le folosește.

Art. 44. — Suporturile se manipulează astfel încât să fie ferite de praf, solvenți, umiditate, temperaturi peste 30°C, acțiunea directă a razelor solare, zgâriere, șocuri mecanice și termice, câmpuri electromagnetice puternice.

Art. 45. — Depozitarea suporturilor trebuie făcută în locuri și în condiții care să respecte indicațiile furnizorilor suporturilor respective și să asigure o securitate fizică corespunzătoare.

Art. 46. — Suporturile trebuie șterse înainte de a fi oferite spre reutilizare. Ștergerea trebuie să fie sigură, astfel încât să facă imposibilă reconstituirea informațiilor înregistrate anterior pe suporturile în cauză, chiar dacă aceste informații nu mai sunt de actualitate.

Art. 47. — Este interzisă utilizarea suporturilor externe de stocare a datelor pentru copierea de fișiere, programe, date obținute din surse nesigure (din afara sistemului informatic al MFP, internet, prieteni, cunoscuți etc.) pe stația de lucru, fără a fi verificate în prealabil cu programul antivirus instalat pe aceasta.

Art. 48. — Transportul suporturilor se asigură numai de persoane autorizate. Suporturile conținând informații sensibile nu pot fi furnizate în afara organizației fără autorizația proprietarului drepturilor asupra datelor respective; autorizația este înregistrată pentru a servi drept dovadă la controlul de audit.

Art. 49. — Transportul suporturilor se asigură astfel încât să se evite pierderea sau furtul, precum și citirea sau copierea de către persoane autorizate.

Art. 50. — Suporturile care conțin informații sensibile vor fi casate prin incinerare, distrugere (zdrobire, tocare).

SECȚIUNEA a 2-a

Reguli în caz de incidente sau defectări

Art. 51. — Incidentele care afectează activitatea normală (violări de securitate, amenințări, vulnerabilități sau defectări), care ar putea avea impact asupra utilizării resurselor din organizație, trebuie raportate conducerii direcției în cel mai scurt timp posibil, aceasta urmând ca împreună cu DGTI și/sau cu furnizorul respectiv de servicii să decidă măsurile necesare remedierii lor.

Art. 52. — Furtul sau vandalizarea stației de lucru, a suporturilor externe de stocare a datelor, pierderea sau copierea neautorizată a suporturilor externe de stocare a datelor, precum și orice alt incident privind stația de lucru ori suporturile externe de stocare a datelor trebuie comunicate imediat conducerii compartimentului (direcției) care, în cel mai scurt timp posibil, trebuie să ia măsurile necesare pentru recuperare, precum și orice alte măsuri prevăzute de lege.

Art. 53. — În funcție de problemele ivite în funcționarea sistemelor sau a serviciilor, remediile vor fi făcute fie de DGTI, fie de către furnizori de servicii, cât mai rapid posibil.

Art. 54. — Orice întârziere în anunțarea vulnerabilităților suspectate poate fi interpretată ca un potențial abuz în utilizarea sistemului și poate atrage măsuri disciplinare.

SECȚIUNEA a 3-a

Raportarea deranjamentelor hardware/software

Art. 55. — La observarea unor deranjamente în funcționarea corectă a resurselor hardware/software, utilizatorul are următoarele obligații:

a) trebuie notat orice simptom al problemei și orice mesaj care apare pe ecran;

b) trebuie izolat calculatorul față de rețea prin deconectarea patch cordului de la priza de rețea, iar, dacă este posibil, utilizarea sa trebuie oprită. Trebuie anunțată imediat persoana de contact corespunzătoare. Dacă echipamentul trebuie examinat, el trebuie deconectat de la orice rețea, inclusiv de la rețeaua electrică. Mediile/Suporturile externe de stocare a datelor nu vor fi transferate la alte calculatoare;

c) personalul desemnat din cadrul DGTI și/sau aparținând furnizorului respectiv de servicii trebuie să se ocupe de refacerea sistemului.

SECȚIUNEA a 4-a

Politica biroului curat și a ecranului curat

Art. 56. — Toți utilizatorii din cadrul MFP trebuie să ia în considerare adoptarea unei „politici de birou curat” atât pentru documentele pe suport tip hârtie, cât și pentru medii/suporturi externe de stocare a datelor. De asemenea, trebuie adoptată politica „ecranului curat” pentru echipamentele de procesare a informației, în scopul reducerii riscului de acces neautorizat, precum și de pierdere sau distrugere a informației în timpul sau în afara orelor de lucru normale.

Art. 57. — Această politică trebuie să țină seama de clasificările de securitate ale informației, precum și de riscurile aferente.

Art. 58. — Acolo unde se consideră necesar, documentele pe suport tip hârtie și mediile/suporturile externe de stocare a datelor trebuie păstrate în dulapuri încuiate și/sau în alte tipuri de mobilier securizat, atunci când nu sunt folosite, mai ales în afara programului de lucru.

Art. 59. — În afara programului normal de lucru, imprimantele și scanerele trebuie protejate față de accesul neautorizat.

Art. 60. — Informațiile confidențiale sau clasificate, după ce sunt imprimate, trebuie ridicate imediat din imprimantă.

Art. 61. — Se va evita încărcarea inutilă a spațiului rezervat pe stația de lucru, pe servere și în sistemul de poștă electronică cu fișiere multimedia de mari dimensiuni și se va proceda la ștergerea periodică a informațiilor perimate.

SECȚIUNEA a 5-a

Reguli de utilizare a stațiilor mobile

Art. 62. — Toate regulile prevăzute la cap. II privind utilizarea stației de lucru, precum și dispozițiile cap. III se aplică și în cazul utilizării unei stații mobile, aceasta din urmă având și funcția de suport extern de stocare a informațiilor.

Art. 63. — Suplimentar, responsabilul stației mobile are următoarele îndatoriri:

a) să păstreze și să transporte cu grijă echipamentul;

b) să verifice că pe echipament sunt marcate numele instituției și numărul de inventar și să păstreze copia fișei de inventar a echipamentului;

c) să creeze datele folosind utilitarul instalat;

d) să salveze datele pe medii externe de stocare a informațiilor sau pe serverele de fișiere și apoi să șteargă aceste date de pe echipament de îndată ce acestea și-au îndeplinit scopul de utilizare;

e) să se asigure că ecranul stației mobile este setat cu screen saver cu pornire automată (protejat de parolă) la 3 minute de inactivitate;

f) după fiecare utilizare a echipamentului în afara rețelei de date a MFP și înainte de reconectarea acestuia în rețeaua de date a MFP, să lanseze programul complet de devirusare instalat.

Art. 64. — Responsabilul stației mobile trebuie să protejeze echipamentul, următoarele activități fiind interzise:

a) să lase echipamentul nesupravegheat sau să îl predea spre utilizare membrilor familiei, unor rude, prieteni, cunoscuți sau altor persoane neautorizate;

b) să stocheze timp îndelungat — mai mult de o lună — aceleași date pe echipament, datele având îndeplinit scopul de utilizare;

c) să păstreze mediile/suporturile externe pe care s-au efectuat copii de siguranță ale aplicațiilor, datelor, programelor

etc. în același loc cu echipamentul (de exemplu: în geanta de protecție a echipamentului).

SECȚIUNEA a 6-a

Măsurile disciplinare

Art. 65. — (1) Încălcarea prezentelor instrucțiuni constituie abatere disciplinară și atrage răspunderea disciplinară, potrivit legii.

(2) Măsurile disciplinare pot include și interzicerea accesului la resursele sistemului informatic.

Art. 66. — Anexele nr. 1 și 2 fac parte integrantă din prezentele instrucțiuni.

*ANEXA Nr. 1
la instrucțiuni*

SECURITATEA sistemelor informatice și a comunicațiilor de date

Procedurile de securitate ale sistemelor informatice se referă la securitatea fizică, hardware, software, de comunicații și la securitatea datelor și informațiilor vehiculate în cadrul acestor sisteme.

SECȚIUNEA 1

Securitatea fizică

Art. 1. — Măsurile pentru prevenirea ori împiedicarea atacurilor asupra resurselor sistemului informatic sunt:

a) echipamentul informatic este distribuit nominal, pe bază de fișă de inventar, salariaților din Ministerul Finanțelor Publice, denumit în continuare *MFP*;

b) ușile sunt încuiate la sfârșitul fiecărei zile și numai personalul autorizat are acces la echipamentele de tehnologia informației și comunicațiilor;

c) stațiile de lucru mobile sunt încuiate în dulapuri la sfârșitul fiecărei zile și numai personalul autorizat are acces la aceste echipamente;

d) serverele funcționează în camere tehnice special amenajate în zone protejate și numai personalul autorizat are acces la aceste echipamente;

e) accesul în instituție se face numai pe bază de legitimație *MFP*;

f) vizitatorii trebuie însoțiți pe parcursul vizitei lor în zonele protejate din instituție;

g) instituția are asigurată paza 24 de ore pe zi, 7 zile pe săptămână;

h) funcționarii care au încetat raporturile de serviciu sau ale căror raporturi de serviciu au fost suspendate nu mai au acces în sediul instituției decât în calitate de vizitatori;

i) administratorul de rețea înregistrează toți vizitatorii la server, iar informațiile despre vizitatori sunt păstrate cel puțin 2 ani;

j) conform Legii nr. 349/2002 pentru prevenirea și combaterea efectelor consumului produselor din tutun, cu modificările și completările ulterioare, fumatul este interzis în spațiile publice închise.

SECȚIUNEA a 2-a

Securitatea hardware

Art. 2. — Responsabilitatea administrării securității hardware-ului depinde de echipamentele utilizate, după cum urmează:

a) fiecare utilizator este responsabil de stația lui de lucru;

b) administratorul de rețea este responsabil de toate echipamentele aferente serverelor deservite din camerele tehnice;

c) fiecare stație de lucru trebuie inventariată și etichetată;

d) toate echipamentele trebuie întreținute conform instrucțiunilor furnizorului;

e) numai personalului autorizat i se permite efectuarea întreținerii ori a reparațiilor;

f) accesul la orice stație de lucru trebuie limitat prin utilizarea de nume de utilizator și parolă;

g) fiecare utilizator final este direct responsabil de gestionarea drepturilor de acces pe stația sa de lucru;

h) parola trebuie să fie sigură, secretă și schimbată regulat;

i) stația altui utilizator final poate fi folosită doar dacă există aprobare pe linie ierarhică;

j) dacă există riscul ca o persoană neautorizată să cunoască parola de acces la o stație de lucru, parola trebuie schimbată;

k) în cazul absenței de la birou a utilizatorului final, acesta trebuie să blocheze în prealabil accesul pe stația sa de lucru;

l) ecranele stațiilor de lucru trebuie setate cu screen saver cu pornire automată (protejat de parolă), cu excepția cazurilor exprese în care superiorul ierarhic dispune altfel;

m) în timpul nopții, stațiile de lucru trebuie închise, exceptând cazurile în care există ordin contrar, scris, al superiorului ierarhic.

SECȚIUNEA a 3-a

Securitatea software

Art. 3. — Măsurile pentru diminuarea vulnerabilității sistemului informatic accesat, a aplicațiilor informatice, precum și pentru eficientizarea operațiilor de lucru:

a) administratorul de rețea este responsabil de instalarea și actualizarea tuturor programelor software pe toate stațiile de lucru din cadrul *MFP*, conform licențelor deținute;

b) administratorul de rețea va lua toate măsurile necesare de respingere a descărcărilor de aplicații neautorizate;

c) administratorul de rețea este responsabil de instalarea și actualizarea utilităților antivirus;

d) utilizatorul este responsabil de utilizarea software-ului instalat;

e) utilizatorilor le este interzisă modificarea configurării stației de lucru, sistemului de operare, rețelei și a serverului accesat;

f) utilizatorilor le este interzisă instalarea aplicațiilor neautorizate;

g) în cazul stațiilor incluse în Active Directory, instalarea aplicațiilor, actualizarea programelor, a sistemului de operare și

configurarea stației de lucru sunt controlate și blocate prin politicile serverului de Domain Controller;

h) utilizatorii trebuie să respecte termenii licențelor referitoare la drepturile de autor, precum și prevederile Legii nr. 8/1996 privind dreptul de autor și drepturile conexe, cu modificările și completările ulterioare; responsabilitatea în cazul încălcării acestei obligații revine utilizatorilor în cauză;

i) utilizatorilor finali le este interzisă îndepărtarea protecției antivirus sau a oricăror altor aplicații; numai administratorul de rețea are această atribuție;

j) pentru protecția sistemului informatic se recomandă ca utilizatorii să nu deschidă niciodată fișiere atașate, recepționate prin e-mail, provenind dintr-o sursă suspectă; se recomandă de asemenea ștergerea acestor fișiere.

SECȚIUNEA a 4-a

Securitatea comunicării

Art. 4. — Securitatea comunicării se referă atât la securitatea comunicării interne, cât și la securitatea comunicării externe: e-mail (poștă electronică) și website. Astfel:

a) administratorul de rețea este responsabil de crearea și menținerea conturilor de e-mail atât pe servere, cât și pe stații, dar fiecare utilizator în parte este responsabil de modul de utilizare și de conținutul propriului cont;

b) utilizatorii sistemului informatic din cadrul MFP nu trebuie să se conecteze la rețele de comunicare neautorizate;

c) utilizatorii trebuie să utilizeze contul lor de e-mail numai în scopuri profesionale, în interes de serviciu, servind în totalitate interesele MFP;

d) prin crearea și trimiterea e-mailurilor, salariații MFP își asumă personal responsabilitatea conținutului respectiv, iar orice opinie sau afirmație în numele ministrului finanțelor publice, al ministerului sau al oricărei altei structuri din aparatul propriu al MFP se va face strict în urma unei autorizări scrise;

e) este obligatoriu ca utilizatorii să se asigure în privința identității corespondentului lor înainte de a comunica orice informație sensibilă sau critică;

f) corespondența în scop de serviciu cu personalul instituțiilor publice se va face numai pe adresele de e-mail din extranet-ul MFP sau, în lipsa acestora, pe adresele de e-mail sau website oficiale ale instituțiilor respective;

g) în cazul corespondenței prin rețele publice (internet) se va ține seama de faptul că nu există garanții privind asigurarea confidențialității și protecției corespondenței;

h) este interzisă transmiterea/retransmiterea de mesaje cu caracter vulgar, injurios, defăimător sau pentru a hărțui persoane;

i) securitatea conturilor de e-mail pe stații este asigurată de aplicații antivirus;

j) este considerată ilegală utilizarea conexiunii internet a organizației pentru alte scopuri decât cele strict legate de îndeplinirea sarcinilor de serviciu;

k) este interzisă accesarea site-urilor rasiste, pornografice sau pedofile;

l) este interzisă încheierea de contracte on-line în numele MFP fără autorizare în acest sens;

m) este interzis a se face achiziții on-line fără autorizare în acest sens;

n) violarea politicilor MFP cu privire la utilizarea poștei electronice va fi comunicată atât forurilor ierarhice superioare din cadrul direcției respective, cât și celor din Direcția de audit public intern și poate fi soldată cu restricționarea accesului la resursele sistemului informatic, dar și cu alte sancțiuni disciplinare, aplicabile conform Legii nr. 188/1999 privind Statutul funcționarilor publici, republicată, cu modificările și completările ulterioare.

SECȚIUNEA a 5-a

Securitatea datelor și a informațiilor

Art. 5. — Sistemul informatic al MFP se bazează pe sistemele de procesare și stocare a datelor electronice; în vederea desfășurării corespunzătoare a activităților din cadrul MFP, precum și a atingerii obiectivelor propuse, este esențial ca aceste sisteme să fie protejate împotriva utilizării, vehiculării și păstrării în condiții impropii și nesigure.

Art. 6. — În acest sens, trebuie respectate prevederile Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare.

Art. 7. — De asemenea, utilizatorii sistemului informatic din cadrul MFP trebuie să țină seama de următoarele aspecte:

a) administratorul este responsabil de securitatea sistemului informatic și a circulației informațiilor la nivel de rețea/servele din cadrul MFP, dar fiecare utilizator final din MFP este responsabil atât pentru informațiile de pe stația sa de lucru, cât și de cele pe care le introduce pe servere prin aplicațiile accesate;

b) un utilizator final nu trebuie să citească, să modifice, să copieze sau să distrugă, direct ori indirect, date care nu îi aparțin; utilizatorul final trebuie să nu transmită aceste date unui destinatar neautorizat;

c) dacă în cursul exercitării sarcinilor de serviciu utilizatorul final accesează accidental informații asupra cărora nu are drept de acces, va comunica superiorului ierarhic momentul exact când aceasta s-a întâmplat și nu va divulga sau propaga aceste informații;

d) în caz de suspiciuni în ceea ce privește compromiterea informațiilor din baza de date, utilizatorul final trebuie să comunice aceste suspiciuni superiorului ierarhic, precum și DGTI, printr-o cerere avizată de către superiorul ierarhic;

e) datele proprii de pe stația de lucru trebuie salvate, utilizatorul final fiind obligat să stabilească și să execute periodic, de comun acord cu conducerea direcției respective, un program de backup al acestora, pe medii de stocare externe stației;

f) mediile/suporturile externe de stocare a datelor ce conțin informații trebuie păstrate în seif sau depuse sub cheie, în funcție de confidențialitatea și importanța datelor respective; utilizatorul final va avea grijă ca mediile/suporturile externe de stocare a datelor să nu se deterioreze și să nu se piardă;

g) informațiile aparținând altor utilizatori, chiar atunci când acestea nu sunt protejate, nu trebuie citite sau copiate;

h) scoaterea din uz a mediilor/suporturilor externe de stocare a datelor se face prin ștergerea datelor și distrugerea fizică a mediilor/suporturilor externe;

i) utilizatorii serviciului de poștă electronică din cadrul MFP trebuie să ia măsurile necesare pentru protejarea datelor vehiculate prin acest serviciu informatic, păstrând confidențialitatea lor conform atribuțiilor de serviciu.

Art. 8. — Dispoziții suplimentare referitoare la incriminarea penală și supravegherea securității datelor, a securității sistemelor informatice și a celor de telecomunicații:

a) pedepsirea abaterilor de la normele de securitate a datelor și a sistemelor electronice se face conform Legii 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;

b) modul de utilizare a poștei informatice din domeniul <mfinate.ro>, a mijloacelor informatice și a rețelelor poate fi auditat de Direcția de audit public intern. În acest sens, trebuie facilitat accesul auditorilor la stațiile de lucru și la servere.

PROCEDURA
pentru asigurarea accesului autorizat la stațiile de lucru și la aplicațiile informatice centralizate
în intranetul Ministerului Finanțelor Publice

CAPITOLUL I

Dispoziții generale

Art. 1. — Prezenta procedură este stabilită în conformitate cu politica Ministerului Finanțelor Publice, denumit în continuare *MFP*, privind asigurarea securității sistemului informatic, de telecomunicații și de protecție a datelor și informațiilor.

Art. 2. — Ținând cont de faptul că fiecare utilizator este responsabil de stația lui de lucru, accesul la stații trebuie limitat prin parolă (fiecare utilizator fiind direct răspunzător de gestionarea drepturilor de acces pe stația sa de lucru). În acest sens se stabilesc următoarele reguli pentru alcătuirea și utilizarea parolei:

- a) utilizatorul trebuie să se asigure că parola este dificil de intuit;
- b) parola este de tip complex: lungimea minimă trebuie să fie de 8 caractere alfanumerice, dintre care minimum o majusculă, minimum o cifră și niciun caracter special (adică de tip „;: ?!@#%&*<> - _ t =);
- c) parola nu poate conține elemente din nume, prenume, cod de identificare, marcă;
- d) perioada maximă de valabilitate a parolei este de 31 de zile;
- e) perioada minimă de valabilitate a parolei este de 15 zile;
- f) numărul minim de parole memorate automat este 3;
- g) numărul maxim de încercări nereușite de înscriere a parolei este 5;
- h) durata blocării accesului după depășirea numărului maxim de încercări nereușite de înscriere a parolei: 30 minute;
- i) parola nu se comunică niciunei alte persoane;
- j) utilizatorul răspunde de utilizarea parolei.

CAPITOLUL II

Procedura aplicată în cazul personalului care nu utilizează sistemul de management al identității <Mgmtld>

Art. 3. — Pentru salariații care nu utilizează sistemul de management al identității <Mgmtld> accesul la stațiile de lucru este controlat de funcțiile de administrare a conturilor utilizatorilor ale sistemelor de operare Windows. Pe măsură ce sistemul de management al identității <Mgmtld> va fi pus în funcțiune, numărul utilizatorilor procedurii se va restrânge.

Art. 4. — Contul utilizatorilor pe stația de lucru este un cod alfanumeric, este stabilit de către administratorul de rețea și este public.

Art. 5. — Reguli privind parola utilizatorului pe stația de lucru:

- a) fiecare utilizator este responsabil de stația sa de lucru;
- b) accesul la stațiile de lucru trebuie limitat prin utilizarea de parole;
- c) parola trebuie ținută secretă ori schimbată regulat;
- d) administrarea parolei este responsabilitatea utilizatorului;
- e) dacă există riscul ca o persoană neautorizată să cunoască parola de acces la stația de lucru, parola trebuie schimbată.

Art. 6. — Schimbarea parolei se face de către utilizator în oricare dintre următoarele situații:

- a) imediat după ce i-a fost comunicată de către o altă persoană;
- b) imediat după preluarea stației de lucru;
- c) la expirarea perioadei de valabilitate.

Schimbarea se face conform Regulilor pentru stabilirea și utilizarea parolei și urmând instrucțiunile pentru crearea și modificarea parolei.

Art. 7. — Schimbarea parolei se face, de asemenea, de către utilizator înainte de expirarea perioadei de valabilitate dacă utilizatorul consideră că parola a devenit cunoscută altei persoane. Utilizatorul trebuie să anunțe despre acest eveniment conducerea direcției. Evenimentul trebuie să fie consemnat de către secretara direcției în Jurnalul de evidență a incidentelor de acces la sistemul informatic întreținut în cadrul direcției. Schimbarea se face de către utilizator în conformitate cu Regulile pentru stabilirea și utilizarea parolei și urmând instrucțiunile pentru crearea și modificarea parolei.

Art. 8. — Schimbarea parolei se face, de asemenea, de către utilizator dacă a depășit numărul maxim de încercări nereușite de înscriere a parolei (a uitat parola). Utilizatorul trebuie să anunțe despre acest eveniment conducerea direcției. Evenimentul trebuie să fie consemnat de către secretara direcției în Jurnalul de evidență a incidentelor de acces la sistemul informatic întreținut în cadrul direcției, apoi utilizatorul trebuie să apeleze la suportul tehnic furnizat de punctul de contact Help desk.

Art. 9. — Solicitarea de asistență pentru schimbarea parolei este consemnată de personalul punctului de contact Help desk în Jurnalul de evidență a incidentelor în sistemul informatic. Administratorul de rețea autorizat să trateze solicitarea accesează stația de lucru la nivel de „administrator” folosind parola adecvată, generează o nouă parolă de acces pentru utilizator și o comunică pe loc acestuia. Accesul la stația de lucru se face numai în prezența și cu acordul utilizatorului stației de lucru. Imediat ce i-a fost comunicată, utilizatorul schimbă parola, urmând instrucțiunile pentru crearea și modificarea parolei, astfel încât să o cunoască numai el. Parola creată de utilizator trebuie să respecte Regulile pentru stabilirea și utilizarea parolei.

Art. 10. — Ori de câte ori se părăsește stația de lucru se închide sesiunea de lucru (aplicația) prin comanda „Log off” și se blochează accesul la stație prin combinația de taste CTRL+ALT+DEL și butonul Lock sau combinația de taste Winkey (tasta Windows)+L.

Art. 11. — Setarea cu screen saver cu pornire automată, protejat prin parolă, se face în panoul „Display Properties/Screen Saver” al monitorului, bifând opțiunea „On resume, password protect”, stabilind un timp de așteptare până la pornirea automată a screen saverului de 3—10 minute prin completarea câmpului „wait minutes” și punând-o în funcțiune cu comanda „Apply”.

CAPITOLUL III

Procedura aplicată în cazul personalului care utilizează sistemul de management al identității <Mgmtld>

Art. 12. — Sistemul de management al identității <Mgmtld> este un nou sistem informatic, care este în curs de implementare și urmează a fi generalizat la nivelul MFP și al instituțiilor subordonate. Are ca scop administrarea în mod centralizat a accesului la toate aplicațiile informatice și posturile de lucru, folosind identificarea sigură a persoanei și un ansamblu de roluri stabilite de personalul îndreptățit.

Art. 13. — Accesul la stațiile de lucru se face diferențiat, după cum utilizatorul stației respective face parte sau nu din Active Directory <AD> (platforma software dedicată administrării stațiilor de lucru care interacționează cu funcțiile de administrare a conturilor utilizatorilor sistemelor de operare Windows) astfel:

- a) cazul stațiilor ai căror utilizatori sunt integrați în <AD>:
 - (i) sistemul de management al identității <Mgmtld> generează o parolă inițială (default) pentru userul în cauză;
 - (ii) Active Directory la rândul său, prin politicile stabilite de către administratorul serverului de Domain Controller, obligă utilizatorul să își schimbe parola la prima logare;
 - (iii) în caz de pierdere a parolei, userul este obligat să apeleze la punctul de contact Help desk și să solicite resetarea parolei. Administratorul de <AD> (sau persoana desemnată în acest sens din cadrul punctului de contact Help desk) va reseta parola, punând o parolă generică și forțând utilizatorul (automat, prin politicile stabilite în <AD>) să o modifice la primul „Log on”;
- b) cazul stațiilor ai căror utilizatori nu sunt integrați în <AD>:
 - (i) sistemul de management al identității <Mgmtld> generează o parolă de acces inițială pentru utilizatorul în cauză, dar nu îl forțează, prin politicile sale, să își schimbe parola la prima logare;
 - (ii) utilizatorul trebuie să respecte normele interne prezente și să procedeze la schimbarea parolei inițiale cu o parolă personală, setată la următorul „Log on”;

c) potrivit strategiei de dezvoltare a sistemului informatic al MFP, sistemul de management al identității <Mgmtld> va fi extins și generalizat.

Art. 14. — Schimbarea parolei se face de către utilizator imediat după primirea/preluarea stației de lucru (la primul „Log on”), astfel încât să o cunoască numai el, conform Regulilor de stabilire și utilizare a parolei.

Art. 15. — Schimbarea parolei se face de către utilizator, la expirarea perioadei de valabilitate a parolei, în conformitate cu Regulile pentru stabilirea și utilizare a parolei.

Art. 16. — Schimbarea parolei se face de către utilizator înainte de expirarea perioadei de valabilitate, dacă el consideră că aceasta a devenit cunoscută altei persoane. Utilizatorul trebuie să anunțe despre acest eveniment conducerea direcției. Evenimentul trebuie să fie consemnat de către secretara direcției în Jurnalul de evidență a incidentelor de acces la sistemul informatic întreținut în cadrul direcției. Schimbarea se

face de către utilizator în conformitate cu Regulile pentru stabilirea și utilizarea parolei. În cazul în care schimbarea se face înainte de expirarea perioadei minime de valabilitate a parolei, utilizatorul trebuie să apeleze la suportul tehnic furnizat de către punctul de contact Help desk.

Ar. 17. — Schimbarea parolei se face de către utilizator dacă a depășit numărul maxim de încercări nereușite de înscriere a parolei (a uitat parola). Utilizatorul trebuie să anunțe despre acest eveniment conducerea direcției. Evenimentul trebuie să fie consemnat de către secretara direcției în Jurnalul de evidență a incidentelor de acces la sistemul informatic întreținut în cadrul direcției, apoi utilizatorul trebuie să apeleze la suportul tehnic furnizat de punctul de contact Help desk.

Art. 18. — Solicitarea de asistență pentru schimbarea parolei este consemnată de personalul punctului de contact Help desk în Jurnalul de evidență a incidentelor în sistemul informatic. Persoana care tratează solicitarea contactează telefonic secretariatul direcției în care este încadrat solicitantul și verifică identitatea solicitantului, precum și dacă evenimentul a fost consemnat în Jurnalul de evidență a incidentelor de acces la sistemul informatic întreținut în cadrul direcției.

Art. 19. — Dacă solicitarea de schimbare a parolei nu este îndreptățită, adică utilizatorul nu este salariat în cadrul direcției sau evenimentul nu este consemnat în Jurnalul de evidență a incidentelor de acces la sistemul informatic întreținut în cadrul direcției, persoana care tratează solicitarea consemnează despre aceasta în Jurnalul de evidență a incidentelor în sistemul informatic, comunică despre aceasta prin poștă electronică internă secretarei direcției, solicitând consemnarea evenimentului și în Jurnalul de evidență a incidentelor de acces la sistemul informatic întreținut în cadrul direcției. Dacă solicitarea de schimbare a parolei nu este îndreptățită, nu se va genera o nouă parolă.

Art. 20. — Dacă solicitarea de schimbare a parolei este îndreptățită, persoana care tratează solicitarea consemnează despre aceasta în Jurnalul de evidență a incidentelor în sistemul informatic și generează imediat o nouă parolă de acces și o comunică de îndată telefonic solicitantului. Parola generată respectă Regulile pentru stabilirea și utilizarea parolei.

Art. 21. — Schimbarea parolei se face de către utilizator, imediat după ce i-a fost comunicată de către punctul de contact Help desk, astfel încât să o cunoască numai el. Parola creată de utilizator trebuie să respecte Regulile pentru stabilirea și utilizarea parolei.

Art. 22. — Schimbarea parolei pe stația de lucru se face de către utilizatorul final prin tastarea combinației de taste CTRL+ALT+DEL și butonul „Change Password”.

Art. 23. — Ori de câte ori se părăsește stația de lucru se închide sesiunea de lucru (aplicația) prin comanda „Log off” și se blochează accesul la stație prin combinația de taste CTRL+ALT+DEL și butonul „Lock” sau combinația de taste Winkey (tasta Windows)+L.

Art. 24. — Setarea cu screen saver cu pornire automată, protejat prin parolă, se face în panoul „Display Properties/Screen Saver” al monitorului, bifând opțiunea „On resume, password protect”, stabilind un timp de așteptare până la pornirea automată a screen saverului de 3—10 minute prin completarea câmpului „wait minutes” și punând-o în funcțiune cu comanda „Apply”.