Ordinul nr. 279/1.736/2012 al ministrului administraţiei şi internelor şi al viceprim-ministrului, ministrul finanţelor publice privind aprobarea modelului-cadru al protocolului de cooperare în vederea schimbului de informaţii între Agenţia Naţională de Administrare Fiscală şi autorităţile publice locale

ART. 1

Pentru realizarea schimbului de informaţii între Agenţia Naţională de Administrare Fiscală şi autorităţile administraţiei 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 dispoziţiilor Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi liberă circulaţie a acestor date, cu modificările şi completările ulterioare.

(2) În accepţiunea art. 3 lit. e) din Legea nr. 677/2001, cu modificările şi completările ulterioare, Agenţia Naţională 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.

ANEXĂ

AGENŢIA NAŢIONALĂ DE ADMINISTRARE FISCALĂ	**UNITATEA/SUBDIVIZIUNEA ADMINISTRATIV-TERITORIALĂ**
Nr. ...../..... 20...	**Nr. ...../..... 20...**

PROTOCOL DE COOPERARE

În temeiul următoarelor prevederi legale:

- Legea administraţiei publice locale nr. 215/2001, republicată, cu modificările şi completările ulterioare;
- Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi liberă circulaţie a acestor date, cu modificările şi completările ulterioare;
- art. 11, 61 şi 62 din Ordonanţa Guvernului nr. 92/2003 privind Codul de procedură fiscală, republicată, cu modificările şi completările ulterioare;

- art. 5 alin. (1) lit. g) din Hotărârea Guvernului nr. 109/2009 privind organizarea şi funcţionarea Agenţiei Naţionale de Administrare Fiscală, cu modificările şi completările ulterioare;

- Hotărârea Guvernului nr. 717/2009 privind aprobarea normelor de implementare a programului "Prima casă", cu modificările şi completările ulterioare;

- Ordinul ministrului finanţelor publice nr. 2.875/2009 pentru aprobarea instrucţiunilor privind utilizarea sistemului informatic din cadrul Ministerului Finanţelor Publice,

- Ordinul ministrului finanţelor publice nr. 551/2003 pentru aprobarea Instrucţiunilor de aplicare a prevederilor titlului I - "Transparenţa informaţiilor referitoare la obligaţiile bugetare restante" al cărţii I din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, cu modificările şi completările ulterioare, privind transparenţa administraţiei publice centrale şi locale şi parteneriat cu cetăţenii;

- Legea nr. 455/2001 privind semnătura electronică;

- Hotărârea Guvernului nr. 1.259/2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, cu modificările ulterioare,

Ministerul Finanţelor Publice, prin Agenţia Naţională de Administrare Fiscală, denumită în continuare ANAF, cu sediul în Bucureşti, str. Apolodor nr. 17, sectorul 5, reprezentată prin domnul ....., în calitate de preşedinte,

şi

Unitatea/subdiviziunea administrativ-teritorială, cu sediul în ....., reprezentată prin domnul ....., în calitate de .....,

denumite în continuare părţi, au convenit la încheierea prezentului protocol.

ART. 1

Obiectul protocolului

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

a) creşterii nivelului de colectare a taxelor şi impozitelor la bugetul general consolidat al statului;

b) prevenirii şi combaterii evaziunii fiscale;

c) facilitării accesului persoanelor fizice şi juridice la informaţii deţinute de instituţiile publice semnatare.

ART. 2

Obligaţiile părţilor

În termen de maximum 30 de zile de la data semnării prezentului protocol părţile vor stabili şi vor semna procedura de lucru comună. Procedura de lucru se va semna la nivelul structurilor tehnice ale celor doua instituţii şi va conţine toate detaliile privind modalitatea de implementare a serviciilor din punct de vedere organizatoric şi procedural.

În îndeplinirea obiectivelor prezentului protocol, cele două părţi semnatare au obligaţia respectării prevederilor referitoare la protejarea secretului fiscal din Ordonanţa Guvernului nr. 92/2003 privind Codul de procedură fiscală, republicată, cu modificările şi completările ulterioare.

2.1. Obligaţiile unităţii/subdiviziunii administrativ-teritoriale

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

a) patrimoniul persoanelor fizice şi juridice (bunuri imobile şi bunuri mobile) şi rolul nominal unic;

b) creanţele datorate de contribuabili (persoane fizice şi juridice) bugetului general al unităţii/subdiviziunii administrativ teritoriale.

2.1.2. Unitatea/Subdiviziunea administrativ-teritorială:

a) va respecta prevederile legale referitoare la protecţia datelor personale şi a informaţiilor fiscale, prin utilizarea informaţiilor din bazele de date ale Ministerului Finanţelor Publice numai în scopurile prevăzute de lege;

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

c) va respecta procedura şi normele de conectare la reţea şi la serviciile oferite de sistemul informatic al Ministerului Finanţelor Publice, stabilite de către Ministerul Finanţelor Publice şi Serviciul de Telecomunicaţii Speciale;

d) va solicita la ANAF înrolarea certificatelor digitale obţinute pentru funcţionari în sistemul de management al identităţii şi rolurilor utilizatorilor sistemului informatic al Ministerului Finanţelor Publice, folosind tabelul din anexa nr. 2. Datele din anexa nr. 2 vor fi centralizate în format electronic de către unităţile/subdiviziunile administrativ-teritoriale şi trimise către Direcţia generală a tehnologiei informaţiei din cadrul Ministerului Finanţelor Publice, în format electronic. În cazul în care informaţiile ce ţin de furnizarea serviciilor, transmise de unităţile/subdiviziunile administrativ-teritoriale, sunt eronate, Ministerul Finanţelor Publice nu are nicio responsabilitate privind întârzierile în activarea/dezactivarea rolurilor;

e) va solicita modificări în ceea ce priveşte identitatea şi rolurile pe care le deţin persoanele titulare de certificate digitale imediat ce acestea sunt necesare, anunţând Direcţia generală a tehnologiei informaţiei din cadrul Ministerului Finanţelor Publice, în vederea modificării/revocării prin formularul din anexa nr. 3;

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

g) va lista şi păstra registrul de evidenţă al accesului, generat automat de serviciul oferit de sistemul informatic al Ministerului Finanţelor Publice;

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

2.2. Obligaţiile ANAF

2.2.1. ANAF va respecta prevederile legale referitoare la protecţia datelor personale şi a informaţiilor fiscale, prin utilizarea informaţiilor din bazele de date ale unităţii/subdiviziunii administrativ-teritoriale numai în scopurile prevăzute de lege.

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

a) deţinerea de conturi bancare;

b) obligaţiile de plată a contribuţiilor sociale, impozitului pe venit şi evidenţa nominală a persoanelor asigurate care au domiciliul fiscal pe raza teritorială a unităţii/subdiviziunii administrativ-teritoriale;

c) veniturile din salarii şi aferente salariilor, precum şi cele din venituri din alte surse obţinute de contribuabili persoane fizice care au domiciliul fiscal pe raza teritorială a unităţii/subdiviziunii administrativ-teritoriale, denumirea şi codul unic de identificare a angajatorului.

2.2.3. Direcţia generală a tehnologiei informaţiei din cadrul Ministerului Finanţelor Publice:

a) va înrola în sistemul de management al identităţii şi rolurilor al Ministerului Finanţelor Publice, în baza solicitărilor făcute de unitatea/subdiviziunea administrativ-teritorială, certificatele digitale şi va acorda drepturi de acces personalului desemnat al unităţii/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 identităţii şi rolurilor al Ministerului Finanţelor Publice;

c) va asigura personalului unităţii/subdiviziunii administrativ-teritoriale instruirea şi asistenţa tehnică necesară operării în serviciile oferite de sistemul informatic al Ministerului Finanţelor Publice, conform procedurilor Ministerului Finanţelor Publice de instruire a personalului şi de soluţionare a incidenţelor în sistemul informatic;

d) va colabora cu Serviciul de Telecomunicaţii Speciale în vederea asigurării accesului securizat al personalului desemnat al unităţilor/subdiviziunilor administrativ-teritoriale la sistemul informatic al Ministerului Finanţelor Publice.

ART. 3

Modalităţi de realizare a schimbului de informaţii

3.1. Schimbul deinformaţii între părţi (actualizarea bazelor de date) se va realiza periodic, cu respectarea legislaţiei în vigoare, conform procedurii de lucru comune.

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

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

ART. 4

Dispoziţii finale

4.1. Datele şi informaţiile furnizate de părţi sunt confidenţiale şi se utilizează şi se păstrează conform prevederilor legale şi normelor interne în vigoare.

4.2. Părţile vor coopera permanent în vederea adoptării unor puncte de vedere comune pentru elaborarea de noi acte normative sau modificarea celor în vigoare ce reglementează domeniul fiscal, precum şi pentru perfecţionarea cooperării.

4.3. Nerespectarea obligaţiilor asumate prin prezentul protocol de către una dintre părţi dă dreptul părţii lezate de a cere rezilierea acestuia.

4.4. Prezentul protocol poate fi modificat sau completat numai cu acordul scris al ambelor părţi, prin act adiţional, care va deveni parte integrantă a prezentului protocol.

4.5. Partea care are iniţiativa modificării şi/sau completării protocolului va transmite celeilalte părţi, spre analiză, propunerile sale motivate.

4.6. Anexele nr. 1-4 fac parte integrantă din prezentul protocol.

4.7. Prezentul protocol intră în vigoare de la data semnării de către ultima parte.

4.8. Prezentul protocol este valabil pe o perioadă nedeterminată, începând cu data semnării acestuia de către ambele părţi.

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

AGENŢIA NAŢIONALĂ DE ADMINISTRARE FISCALĂ	UNITATEA ADMINISTRATIV-TERITORIALĂ/ SUBDIVIZIUNEA ADMINISTRATIV-TERITORIALĂ
Preşedinte,	Reprezentant,
.....	.....

ANEXA 1
la protocol

AGENŢIA NAŢIONALĂ DE ADMINISTRARE FISCALĂ

Solicitare actualizare utilizatori servicii oferite de sistemul informatic al Primăriei .....

Prin prezenta, vă solicităm dreptul de acces pentru funcţionarii Agenţiei Naţionale de Administrare Fiscală la serviciile oferite de sistemul informatic al Primăriei .....

Numele	Prenumele	Codul numeric personal	E-mail	Telefon	Componenta aplicaţie	Tipul operaţiei

LEGENDA
Tipul operaţiei: consultare
Componenta aplicaţie: IMPOZITE ŞI TAXE LOCALE
Tipul accesului la sistemul informatic al primăriei, prin reţea securizată de STS..... (alte situaţii)

Agenţia Naţională de Administrare Fiscală
Preşedinte .....,
(numele, prenumele şi semnătura)

Data
.....

Solicitările de useri, pentru evidenţa utilizatorilor, se trimit la adresa de e-mail a Primăriei .....

ANEXA 2
la protocol

Instituţia .....

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

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

Numele	Prenumele	Codul numeric personal	E-mail	Telefon	Componenta aplicaţie	Tipul operaţiei

LEGENDA
Tipul operaţiei: consultare
Componenta aplicaţie: ASIGSOC; ASIGSOC/BĂNCI; PATRIMONIU; TRASABILITATE
Tipul accesului la sistemul informatic al Ministerului Finanţelor Publice, prin reţea securizată de STS ..... (alte situaţii)

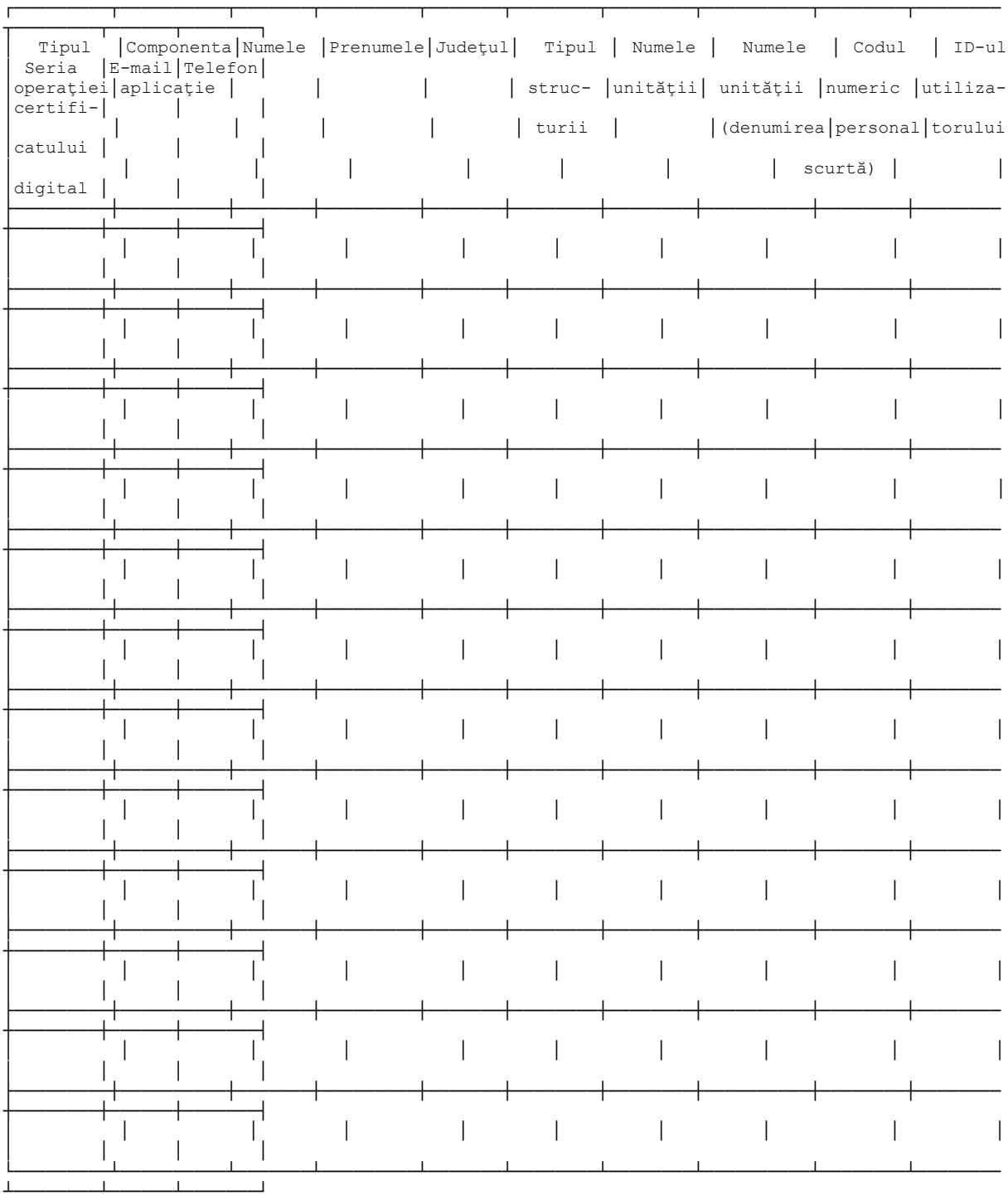
Data Primar
.....
(numele, prenumele şi semnătura)

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

ANEXA Nr. 3
la protocol

Instituţia .....

Modificare/Ştergere drepturi utilizatori servicii oferite de
sistemul informatic al Ministerului Finanţelor Publice



LEGENDĂ

Tipul operaţiei: modificare; ştergere

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

Tipul structurii: felul primăriei, cu reţea securizată sau fără

Judeţul: pentru central, municipiul Bucureşti

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

ANEXA 4
la protocol

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

INSTRUCŢIUNI
privind utilizarea sistemului informatic din cadrul Ministerului Finanţelor Publice

CAP. I
Dispoziţii generale

ART. 1

Prezentele instrucţiuni sunt elaborate în scopul asigurării securităţii informaţiilor în format electronic din cadrul Ministerului Finanţelor Publice, denumit în continuare MFP, şi stabilesc reguli privind protejarea sistemului informatic al ministerului, conform legislaţiei române în vigoare, precum şi convenţiilor internaţionale şi 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 securităţii informaţionale).

ART. 2

În sensul prezentelor instrucţiuni, termenii de mai jos au următoarele definiţii:

a) administrator de reţea - persoană calificată în domeniul tehnologiei informaţiei, desemnată să gestioneze utilizatorii finali, resursele hardware şi software şi modul de acces la resursele reţelei de date;

b) blocare acces staţie de lucru - set de comenzi specific staţiei de lucru care permite interzicerea imediată a accesului de la tastatură la staţia de lucru;

c) dispozitiv wireless - echipament de tehnică de calcul şi comunicaţii care poate asigura conectarea la reţele de comunicaţii prin unde radio;

d) echipamente periferice - imprimantele, scanerele, multifuncţionalele, unităţile mobile disc flexibil, unităţile mobile hard disk, modemurile;

e) fişier multimedia - fişier având o organizare internă dedicată stocării unei combinaţii de formate text, audio, fotografie, animaţie, film şi conţinut 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 (şir de caractere) primit odată cu staţia/aplicaţia, 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 reţea care face legătura între staţie şi priza de reţea montată pe perete;

j) proprietar al drepturilor asupra informaţiilor - persoana angajată sau numită într-o funcţie publică în cadrul MFP care are responsabilitatea stabilirii şi urmăririi regulilor de utilizare şi gestionare a datelor stocate sau prelucrate printr-un serviciu informatic, precum şi de stabilire a condiţiilor de schimb de informaţii cu alte organizaţii;

k) resursele sistemului informatic - echipamentele de tehnologia informaţiei (servere, staţii de lucru, imprimante, scanere etc.), reţelele de comunicaţii de date LAN, MAN, WAN, alte componente şi instalaţii (climatizare, alimentare cu energie, stingere incendiu, control acces fizic etc.), mediile de stocare a datelor, software-ul de bază, aplicaţiile informatice, programele utilitare, datele, bazale de date, fişierele, sistemele de protecţie a datelor, personalul ce exploatează şi întreţine resursele sistemului informatic, documentaţiile de proiectare, documentaţiile de exploatare etc., procedurile de lucru, planurile de continuitate, teoriile ce stau la baza algoritmilor de prelucrare etc.;

l) responsabil cu alimentarea electrică - Direcţia generală de investiţii, achiziţii publice şi servicii interne şi compartimentele din instituţiile publice subordonate aflate în coordonarea sa metodologică;

m) responsabil cu întreţinerea echipamentelor TIC - Direcţia generală a tehnologiei informaţiei, denumită în continuare DGTI, şi compartimentele din instituţiile publice subordonate aflate în coordonarea sa metodologică;

n) reţea de date/reţea de comunicaţii de date - subansamblu al sistemului informatic format din patch corduri, prize de reţea, cablaj structurat, echipamente de comunicaţii, protocoale de comunicaţii şi software pentru administrarea comunicaţiilor. Reţeaua de date are rolul de a oferi suport hardware şi software pentru interconectarea staţiilor de lucru, serverelor, imprimantelor etc. şi pentru acces la serviciile informatice, inclusiv la poştă electronică şi internet;

o) serviciu informatic - unul sau mai multe subsisteme ale sistemului informatic care permit desfăşurarea unui proces de lucru în cadrul organizaţiei;

p) sistemul de management al identităţii <Mgmtld> - sistem centralizat de autentificare a utilizatorilor şi management al drepturilor de acces ale utilizatorilor la resursele sistemului informatic;

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

r) staţie de lucru - ansamblul format din calculator şi echipamentele periferice destinat realizării sarcinilor de serviciu, conectat sau nu la reţeaua de date a MFP şi care are sau nu acces la alte resurse ale sistemului informatic;

s) staţie de lucru mobilă/staţie 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 reţeaua publică;

u) utilizatorul final/responsabilul staţiei de lucru - persoana angajată sau numită într-o funcţie publică în cadrul MFP, care a primit dreptul de acces la staţia de lucru şi drepturi de utilizare a resurselor sistemului informatic.

CAP. II
Reguli de utilizare a staţiei de lucru

SECŢIUNEA 1
Întreţinerea şi urmărirea stării de funcţionare a staţiei de lucru

ART. 3

Staţia de lucru se utilizează în conformitate cu instrucţiunile specifice primite de responsabilul staţiei de lucru odată cu echipamentul.

ART. 4

Pentru a asigura buna funcţionare a staţiei, responsabilul staţiei de lucru are următoarele îndatoriri:

a) să verifice că în exterior, pe carcasa staţiei de lucru, sunt marcate numele instituţiei şi numărul de inventar şi să păstreze copia fişei de inventar a staţiei de lucru, precum şi a celorlalte echipamente de calcul aflate în inventarul său;

b) să amplaseze staţia astfel încât să poată fi utilizată cu uşurinţă şi totodată ferită de lovirea accidentală, de şocuri şi vibraţii, ferită de acţiunea directă a razelor solare, ferită de praf, fum, ploaie şi umezeală;

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

d) să poziţioneze staţia în aşa fel încât cablurile să fie protejate;

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

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

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

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

i) să nu folosească prizele şi prelungitoarele de alimentare pentru staţia de lucru la alimentarea altor consumatori: aparate de aer condiţionat, fierbătoare, frigidere, aspiratoare etc.;

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

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

m) dacă există echipamente periferice, să le urmărească funcţionarea şi să cunoască semnalele de avertizare în caz de funcţionare incorectă a acestora;

n) dacă există unităţi disc flexibil, CD sau DVD, să utilizeze discuri curate, fără urme de deteriorare mecanică, să utilizeze butoanele de deschidere a unităţii disc flexibil, CD sau DVD şi să nu forţeze suportul disc flexibil, CD, DVD prin împingere sau tragere;

o) să sesizeze de urgenţă defectele observate, în funcţie de specificul defecţiunii, responsabilului cu alimentarea electrică sau punctului de contact Help desk;

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

q) să sprijine personalul abilitat pentru remedierea defecţiunilor, furnizând informaţii privind anomaliile de funcţionare observate;

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

ART. 5

Responsabilul staţiei de lucru trebuie să protejeze staţia de lucru, următoarele activităţi fiind interzise:

a) să realizeze conexiuni între echipamentele de calcul, altele decât cele realizate de administratorul de reţea şi responsabilul cu întreţinerea echipamentelor TIC;
b) să schimbe prizele de reţea;
c) să schimbe echipamentele periferice;
d) să înlocuiască monitorul, mouse-ul sau tastatura;
e) să apropriestaţia de surse de încălzire la o distanţă mai mică de 1 m;
f) să obtureze sistemul de ventilaţie al staţiei de lucru;
g) să menţină staţia în funcţiune la temperaturi ale mediului ambiant mai mari de 35 grade Celsius;
h) să utilizeze în apropierea staţiei substanţe chimice corozive, toxice sau inflamabile;
i) să utilizeze staţia cu mâinile ude sau murdare;
j) să lovească staţia sau să o supună şocurilor ori vibraţiilor;
k) să depoziteze obiecte pe echipamente ori pe cabluri;
l) să mănânce, să bea la o distanţă mai mică de 1 m de staţie sau să fumeze în încăperea în care se află staţia.

SECŢIUNEA a 2-a
Politica de utilizare a informaţiilor din MFP

ART. 6
Informaţiile stocate în sistemul informatic, precum şi informaţiile privind sistemul informatic şi resursele acestuia, inclusiv configurarea, organizarea, dezvoltarea şi exploatarea sa, sunt proprietatea MFP, utilizatorul neavând dreptul de a pretinde asigurarea confidenţialităţii sau intimităţii 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 informaţiile din sistemul informatic al MFP pot fi interceptate, monitorizate, controlate, analizate şi arhivate de administratorii de reţea numai în conformitate cu sarcinile de serviciu.
ART. 9
Lucrările cu caracter personal se pot efectua folosind resursele MFP numai cu acordul conducerii direcţiei în care utilizatorul îşi desfăşoară activitatea.
ART. 10
Nu se vor stoca sau prelucra în sistemul informatic al MFP informaţii care nu au legătură cu sarcinile de serviciu.
ART. 11
Utilizatorii sunt obligaţi să respecte măsurile prevăzute în anexa nr. 1 "Securitatea sistemelor informatice şi a comunicaţiilor de date".

SECŢIUNEA a 3-a
Accesul la serviciile staţiei de lucru şi ale sistemului informatic

ART. 12
Dreptul de acces la staţie şi/sau la sistemul informatic îl are numai persoana nominalizată drept utilizator final.

ART. 13

Administratorii de reţea au acces la staţia de lucru a unui utilizator ca urmare a solicitării utilizatorului sau cu ocazia desfăşurării activităţii de mentenanţă ori în alte situaţii aprobate de conducerea MFP sau a direcţiei, după caz.

ART. 14

Drepturile de acces la informaţiile de pe serverele din reţea se vor acorda de către DGTI conform regulilor stabilite de proprietarul drepturilor asupra informaţiilor, în baza unei cereri scrise a conducătorului direcţiei solicitantului şi aprobate de proprietarul drepturilor asupra informaţiilor.

ART. 15

Proprietarul drepturilor asupra informaţiilor stabileşte scopul şi drepturile de utilizare a informaţiilor şi serviciilor informatice, precum şi regulile de protejare şi manipulare a informaţiilor.

ART. 16

Proprietarul drepturilor asupra informaţiilor stabileşte împreună cu DGTI controale adecvate pentru a detecta eventuale încălcări ale regulilor de protejare şi manipulare a informaţiilor.

ART. 17

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

ART. 18

Accesul la staţie se va face utilizând un nume de utilizator (user name) şi o parolă de acces (password), care vor fi cunoscute numai de responsabilul staţiei.

ART. 19

Responsabilul staţiei nu trebuie să permită accesul altor utilizatori la staţia de care răspunde.

ART. 20

Drepturile de acces la nivel de staţie vor fi permise utilizatorului numai de tip limitat, nu şi drepturi de administrare.

ART. 21

Accesul de tip "administrator" la nivel de staţie se va face numai de către administratorul de reţea autorizat, care trebuie să cunoască parola adecvată.

ART. 22

Utilizatorii sunt obligaţi să respecte Procedura pentru asigurarea accesului autorizat la staţiile de lucru şi la aplicaţiile informatice centralizate în intranetul Ministerului Finanţelor Publice, prevăzută în anexa nr. 2.

ART. 23

În reţeaua de date a MFP pot fi conectate numai echipamentele proprietatea MFP, configurate de administratorul de reţea.

ART. 24

Este interzisă conectarea în reţeaua 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 reţeaua de date a MFP de echipamente care nu au fost configurate de administratorul de reţea.

SECŢIUNEA 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 afişa 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 aceştia se oferă să îi ajute în utilizarea staţiei de lucru;

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

d) dacă trebuie să lucreze pe o altă staţie decât cea pentru care este responsabil, el va folosi propriul nume de utilizator (user name) şi parola de acces (password) proprie pentru a accesa această staţie, dacă aceasta este într-un domeniu; în caz contrar, administratorul de reţea 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 staţiei de lucru ori de câte ori este obligat să se deplaseze de lângă aceasta;

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

SECŢIUNEA a 5-a

Securitatea şi protecţia software-ului şi a informaţiilor de pe staţia de lucru

ART. 27

Utilizatorul trebuie să cunoască modul de operare/utilizare, pornire/oprire a staţiei de lucru, precum şi modul de utilizare a aplicaţiilor necesare desfăşurării activităţilor curente din cadrul direcţiei în care activează.

ART. 28

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

ART. 29

Întreţinerea, refacerea, reinstalarea, depanarea software sau/şi hardware în vederea funcţionarii corecte a sistemului de operare şi a aplicaţiilor 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 şi telecomunicaţii ale MFP a oricărei/oricărui aplicaţii, 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 licenţă validă şi aprobate de MFP pot fi instalate pe echipamentele de calcul şi telecomunicaţii 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 investigaţii oficiale.

ART. 34

Pentru protecţia împotriva atacurilor informatice este necesară activarea aplicaţiei de tip firewall de pe staţiile de lucru.

ART. 35

În cazul suspiciunii de infectare informatică, utilizatorul final nu are dreptul să acţioneze din proprie iniţiativă. El trebuie să oprească utilizarea echipamentului în cauză, să îl lase în starea în care acesta se găseşte şi să informeze punctul de contact Help desk al DGTI. Deparazitarea/Ştergerea fişierelor infectate detectate se va realiza de personalul de specialitate al DGTI.

ART. 36

Utilizatorul nu are voie să oprească sau să dezinstaleze programul de protecţie antivirus şi 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 şi nu se vor salva fişiere din internet dacă programul de protecţie antivirus este oprit.

ART. 38

În cazul în care foloseşte programe fără înştiinţarea şi aprobarea DGTI, utilizatorul este direct răspunzător de efectele produse de încălcarea Legii nr. 8/1996 privind dreptul de autor şi drepturile conexe, cu modificările şi completările ulterioare.

ART. 39

Numai proprietarul drepturilor asupra informaţiilor poate autoriza ieşirea datelor din birou sau din sediu ori transmiterea datelor în afara organizaţiei.

ART. 40

Înainte de predarea definitivă a staţiei de lucru, responsabilul acesteia este obligat să salveze toate datele utile pe medii/suporturi externe de stocare a datelor şi apoi să şteargă toate informaţiile de pe staţia 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 informaţii utile şefului său ierarhic.

ART. 42

În scopul prevenirii eventualelor neglijenţe sau a acţiunilor răuvoitoare, în cazul reutilizării staţiilor de lucru sau în cazul casării acestora, serviciul sau direcţia proprietară a datelor va comunica DGTI gradul de confidenţialitate al informaţiilor stocate, hotărând, după caz:

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

b) autorizarea reutilizării staţiilor de lucru după un control prealabil: ştergerea sigură a configuraţiilor, ştergerea sigură a datelor prin rescrierea repetată a suportului.

CAP. III
Alte dispoziţii

SECŢIUNEA 1
Reguli pentru stocarea şi transportul suporturilor externe de stocare a datelor

ART. 43

Suporturile externe de stocare a datelor se inscripţionează de utilizatorul staţiei de lucru cu numele instituţiei şi al compartimentului (direcţiei) care le foloseşte.

ART. 44

Suporturile se manipulează astfel încât să fie ferite de praf, solvenţi, umiditate, temperaturi peste 30°C, acţiunea directă a razelor solare, zgâriere, şocuri mecanice şi termice, câmpuri electromagnetice puternice.

ART. 45

Depozitarea suporturilor trebuie făcută în locuri şi în condiţii care să respecte indicaţiile furnizorilor suporturilor respective şi să asigure o securitate fizică corespunzătoare.

ART. 46

Suporturile trebuie şterse înainte de a fi oferite spre reutilizare. Ştergerea trebuie să fie sigură, astfel încât să facă imposibilă reconstituirea informaţiilor înregistrate anterior pe suporturile în cauză, chiar dacă aceste informaţii nu mai sunt de actualitate.

ART. 47

Este interzisă utilizarea suporturilor externe de stocare a datelor pentru copierea de fişiere, programe, date obţinute din surse nesigure (din afara sistemului informatic al MFP, internet, prieteni, cunoscuţi etc.) pe staţia 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 conţinând informaţii sensibile nu pot fi furnizate în afara organizaţiei fără autorizaţia proprietarului drepturilor asupra datelor respective; autorizaţia 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 şi citirea sau copierea de către persoane autorizate.

ART. 50

Suporturile care conţin informaţii sensibile vor fi casate prin incinerare, distrugere (zdrobire, tocare).

SECŢIUNEA a 2-a
Reguli în caz de incidente sau defectări

ART. 51

Incidentele care afectează activitatea normală (violări de securitate, ameninţări, vulnerabilităţi sau defectări), care ar putea avea impact asupra utilizării resurselor din organizaţie, trebuie raportate conducerii direcţiei în cel mai scurt timp posibil, aceasta urmând ca împreună cu DGTI şi/sau cu furnizorul respectiv de servicii să decidă măsurile necesare remedierii lor.

ART. 52

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

ART. 53

În funcţie de problemele ivite în funcţionarea sistemelor sau a serviciilor, remedierile vor fi făcute fie de DGTI, fie de către furnizori de servicii, cât mai rapid posibil.

ART. 54

Orice întârziere în anunţarea vulnerabilităţilor suspectate poate fi interpretată ca un potenţial abuz în utilizarea sistemului şi poate atrage măsuri disciplinare.

SECŢIUNEA a 3-a
Raportarea deranjamentelor hardware/software

ART. 55

La observarea unor deranjamente în funcţionarea corectă a resurselor hardware/software, utilizatorul are următoarele obligaţii:

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

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

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

SECŢIUNEA a 4-a
Politica biroului curat şi a ecranului curat

ART. 56

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

ART. 57

Această politică trebuie să ţină seama de clasificările de securitate ale informaţiei, precum şi de riscurile aferente.

ART. 58

Acolo unde se consideră necesar, documentele pe suport tip hârtie şi mediile/suporturile externe de stocare a datelor trebuie păstrate în dulapuri încuiate şi/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 şi scanerele trebuie protejate faţă de accesul neautorizat.

ART. 60

Informaţiile confidenţiale sau clasificate, după ce sunt imprimate, trebuie ridicate imediat din imprimantă.

ART. 61

Se va evita încărcarea inutilă a spaţiului rezervat pe staţia de lucru, pe servere şi în sistemul de poştă electronică cu fişiere multimedia de mari dimensiuni şi se va proceda la ştergerea periodică a informaţiilor perimate.

SECŢIUNEA a 5-a
Reguli de utilizare a staţiilor mobile

ART. 62

Toate regulile prevăzute la cap. II privind utilizarea staţiei de lucru, precum şi dispoziţiile cap. III se aplică şi în cazul utilizării unei staţii mobile, aceasta din urmă având şi funcţia de suport extern de stocare a informaţiilor.

ART. 63

Suplimentar, responsabilul staţiei mobile are următoarele îndatoriri:

a) să păstreze şi să transporte cu grijă echipamentul;

b) să verifice că pe echipament sunt marcate numele instituţiei şi numărul de inventar şi să păstreze copia fişei de inventar a echipamentului;

c) să cripteze datele folosind utilitarul instalat;

d) să salveze datele pe medii externe de stocare a informaţiilor sau pe serverele de fişiere şi apoi să şteargă aceste date de pe echipament de îndată ce acestea şi-au îndeplinit scopul de utilizare;

e) să se asigure că ecranul staţiei 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 reţelei de date a MFP şi înainte de reconectarea acestuia în reţeaua de date a MFP, să lanseze programul complet de devirusare instalat.

ART. 64

Responsabilul staţiei mobile trebuie să protejeze echipamentul, următoarele activităţi fiind interzise:

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

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

c) să păstreze mediile/suporturile externe pe care s-au efectuat copiile de siguranţă ale aplicaţiilor, datelor, programelor etc. în acelaşi loc cu echipamentul (de exemplu: în geanta de protecţie a echipamentului).

SECŢIUNEA a 6-a
Măsuri disciplinare

ART. 65

(1) Încălcarea prezentelor instrucţiuni constituie abatere disciplinară şi atrage răspunderea disciplinară, potrivit legii.

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

ART. 66

Anexele nr. 1 şi 2 fac parte integrantă din prezentele instrucţiuni.

ANEXA 1
la instrucţiuni

SECURITATEA
sistemelor informatice şi a comunicaţiilor de date

Procedurile de securitate ale sistemelor informatice se referă la securitatea fizică, hardware, software, de comunicaţii şi la securitatea datelor şi informaţiilor vehiculate în cadrul acestor sisteme.

SECŢIUNEA 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 fişă de inventar, salariaţilor din Ministerul Finanţelor Publice, denumit în continuare MFP;

b) uşile sunt încuiate la sfârşitul fiecărei zile şi numai personalul autorizat are acces la echipamentele de tehnologia informaţiei şi comunicaţiilor;

c) staţiile de lucru mobile sunt încuiate în dulapuri la sfârşitul fiecărei zile şi numai personalul autorizat are acces la aceste echipamente;

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

e) accesul în instituţie se face numai pe bază de legitimaţie MFP;

f) vizitatorii trebuie însoţiţi pe parcursul vizitei lor în zonele protejate din instituţie;

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

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

i) administratorul de reţea înregistrează toţi vizitatorii la server, iar informaţiile despre vizitatori sunt păstrate cel puţin 2 ani;

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

SECŢIUNEA a 2-a
Securitatea hardware

ART. 2
Responsabilitatea administrării securităţii hardware-ului depinde de echipamentele utilizate, după cum urmează:

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

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

c) fiecare staţie de lucru trebuie inventariată şi etichetată;

d) toate echipamentele trebuie întreţinute conform instrucţiunilor furnizorului;

e) numai personalului autorizat i se permite efectuarea întreţinerii ori a reparaţiilor;

f) accesul la orice staţie de lucru trebuie limitat prin utilizarea de nume de utilizator şi parolă;

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

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

i) staţia 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 staţie de lucru, parola trebuie schimbată;

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

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

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

SECŢIUNEA a 3-a
Securitatea software

ART. 3

Măsurile pentru diminuarea vulnerabilităţii sistemului informatic accesat, a aplicaţiilor informatice, precum şi pentru eficientizarea operaţiilor de lucru:

a) administratorul de reţea este responsabil de instalarea şi actualizarea tuturor programelor software pe toate staţiile de lucru din cadrul MFP, conform licenţelor deţinute;

b) administratorul de reţea va lua toate măsurile necesare de respingere a descărcărilor de aplicaţii neautorizate;

c) administratorul de reţea este responsabil de instalarea şi actualizarea utilitarelor antivirus;

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

e) utilizatorilor le este interzisă modificarea configurării staţiei de lucru, sistemului de operare, reţelei şi a serverului accesat;

f) utilizatorilor le este interzisă instalarea aplicaţiilor neautorizate;

g) în cazul staţiilor incluse în Active Directory, instalarea aplicaţiilor, actualizarea programelor, a sistemului de operare şi configurarea staţiei de lucru sunt controlate şi blocate prin politicile serverului de Domain Controller;

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

i) utilizatorilor finali le este interzisă îndepărtarea protecţiei antivirus sau a oricăror altor aplicaţii; numai administratorul de reţea are această atribuţie;

j) pentru protecţia sistemului informatic se recomandă ca utilizatorii să nu deschidă niciodată fişiere ataşate, recepţionate prin e-mail, provenind dintr-o sursă suspectă; se recomandă de asemenea ştergerea acestor fişiere.

SECŢIUNEA a 4-a
Securitatea comunicării

ART. 4

Securitatea comunicării se referă atât la securitatea comunicării interne, cât şi la securitatea comunicării externe: e-mail (poştă electronică) şi website. Astfel:

a) administratorul de reţea este responsabil de crearea şi menţinerea conturilor de e-mail atât pe servere, cât şi pe staţii, dar fiecare utilizator în parte este responsabil de modul de utilizare şi de conţinutul propriului cont;

b) utilizatorii sistemului informatic din cadrul MFP nu trebuie să se conecteze la reţele 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 şi trimiterea e-mailurilor, salariaţii MFP îşi asumă personal responsabilitatea conţinutului respectiv, iar orice opinie sau afirmaţie în numele ministrului finanţelor 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 privinţa identităţii corespondentului lor înainte de a comunica orice informaţie sensibilă sau critică;

f) corespondenţa în scop de serviciu cu personalul instituţiilor 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 instituţiilor respective;

g) în cazul corespondenţei prin reţele publice (internet) se va ţine seama de faptul că nu există garanţii privind asigurarea confidenţialităţii şi protecţiei corespondenţei;

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

i) securitatea conturilor de e-mail pe staţii este asigurată de aplicaţii antivirus;

j) este considerată ilegală utilizarea conexiunii internet a organizaţiei 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 achiziţii on-line fără autorizare în acest sens;

n) violarea politicilor MFP cu privire la utilizarea poştei electronice va fi comunicată atât forurilor ierarhice superioare din cadrul direcţiei respective, cât şi celor din Direcţia de audit public intern şi poate fi soldată cu restricţionarea accesului la resursele sistemului informatic, dar şi cu alte sancţiuni disciplinare, aplicabile conform Legii nr. 188/1999 privind Statutul funcţionarilor publici, republicată, cu modificările şi completările ulterioare.

SECŢIUNEA a 5-a
Securitatea datelor şi a informaţiilor

ART. 5

Sistemul informatic al MFP se bazează pe sistemele de procesare şi stocare a datelor electronice; în vederea desfăşurării corespunzătoare a activităţilor din cadrul MFP, precum şi a atingerii obiectivelor propuse, este esenţial ca aceste sisteme să fie protejate împotriva utilizării, vehiculării şi păstrării în condiţii improprii şi nesigure.

ART. 6

În acest sens, trebuie respectate prevederile Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare.

ART. 7

De asemenea, utilizatorii sistemului informatic din cadrul MFP trebuie să ţină seama de următoarele aspecte:

a) administratorul este responsabil de securitatea sistemului informatic şi a circulaţiei informaţiilor la nivel de reţea/servere din cadrul MFP, dar fiecare utilizator final din MFP este responsabil atât pentru informaţiile de pe staţia sa de lucru, cât şi de cele pe care le introduce pe servere prin aplicaţiile accesate;

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

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

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

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

f) mediile/suporturile externe de stocare a datelor ce conţin informaţii trebuie păstrate în seif sau depuse sub cheie, în funcţie de confidenţialitatea şi importanţa datelor respective; utilizatorul final va avea grijă ca mediile/suporturile externe de stocare a datelor să nu se deterioreze şi să nu se piardă;

g) informaţiile aparţinând 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 ştergerea datelor şi distrugerea fizică a mediilor/suporturilor externe;

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

ART. 8

Dispoziţii suplimentare referitoare la incriminarea penală şi supravegherea securităţii datelor, a securităţii sistemelor informatice şi a celor de telecomunicaţii:

a) pedepsirea abaterilor de la normele de securitate a datelor şi a sistemelor electronice se face conform Legii nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, cu modificările şi completările ulterioare;

b) modul de utilizare a poştei informatice din domeniul <mfinante.ro>, a mijloacelor informatice şi a reţelelor poate fi auditat de Direcţia de audit public intern. În acest sens, trebuie facilitat accesul auditorilor la staţiile de lucru şi la servere.

ANEXA 2
la instrucţiuni

PROCEDURA
pentru asigurarea accesului autorizat la staţiile de lucru şi la aplicaţiile informatice centralizate în intranetul Ministerului Finanţelor Publice

CAP. I
Dispoziţii generale

ART. 1
Prezenta procedură este stabilită în conformitate cu politica Ministerului Finanţelor Publice, denumit în continuare MFP, privind asigurarea securităţii sistemului informatic, de telecomunicaţii şi de protecţie a datelor şi informaţiilor.

ART. 2
Ţinând cont de faptul că fiecare utilizator este responsabil de staţia lui de lucru, accesul la staţii trebuie limitat prin parolă (fiecare utilizator fiind direct răspunzător de gestionarea drepturilor de acces pe staţia sa de lucru). În acest sens se stabilesc următoarele reguli pentru alcătuirea şi 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 şi niciun caracter special (adică de tip .,;:?!@#$%*<>-_t=);

c) parola nu poate conţine 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 nereuşite de înscriere a parolei este 5;

h) durata blocării accesului după depăşirea numărului maxim de încercări nereuşite de înscriere a parolei: 30 minute;

i) parola nu se comunică niciunei alte pesoane;

j) utilizatorul răspunde de utilizarea parolei.

CAP. II
Procedură aplicată în cazul personalului care nu utilizează sistemul de management al identităţii <Mgmtld>

ART. 3
Pentru salariaţii care nu utilizează sistemul de management al identităţii <Mgmtld> accesul la staţiile de lucru este controlat de funcţiile de administrare a conturilor utilizatorilor ale sistemelor de operare Windows. Pe măsură ce sistemul de management al identităţii <Mgmtld> va fi pus în funcţiune, numărul utilizatorilor procedurii se va restrânge.

ART. 4
Contul utilizatorilor pe staţia de lucru este un cod alfanumeric, este stabilit de către administratorul de reţea şi este public.

ART. 5
Reguli privind parola utilizatorului pe staţia de lucru:

a) fiecare utilizator este responsabil de staţia sa de lucru;

b) accesul la staţiile de lucru trebuie limitat prin utilizarea de parole;

c) parola trebuie ţinută secretă ori schimbată regulat;

d) administrarea parolei este responsabilitatea utilizatorului;

e) dacă există riscul ca o persoană neautorizată să cunoască parola de acces la staţia de lucru, parola trebuie schimbată.

ART. 6
Schimbarea parolei se face de către utilizator în oricare dintre următoarele situaţii:

a) imediat după ce i-a fost comunicată de către o altă persoană;

b) imediat după preluarea staţiei de lucru;

c) la expirarea perioadei de valabilitate.

Schimbarea se face conform Regulilor pentru stabilirea şi utilizarea parolei şi urmând instrucţiunile pentru crearea şi 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 anunţe despre acest eveniment conducerea direcţiei. Evenimentul trebuie să fie consemnat de către secretara direcţiei în Jurnalul de evidenţă a incidentelor de acces la sistemul informatic întreţinut în cadrul direcţiei. Schimbarea se face de către utilizator în conformitate cu Regulile pentru stabilirea şi utilizarea parolei şi urmând instrucţiunile pentru crearea şi modificarea parolei.

ART. 8

Schimbarea parolei de face, de asemenea, de către utilizator dacă a depăşit numărul maxim de încercări nereuşite de înscriere a parolei (a uitat parola). Utilizatorul trebuie să anunţe despre acest eveniment conducerea direcţiei. Evenimentul trebuie să fie consemnat de către secretara direcţiei în Jurnalul de evidenţă a incidentelor de acces la sistemul informatic întreţinut în cadrul direcţiei, apoi utilizatorul trebuie să apeleze la suportul tehnic furnizat de punctul de contact Help desk.

ART. 9

Solicitarea de asistenţă pentru schimbarea parolei este consemnată de personalul punctului de contact Help desk în Jurnalul de evidenţă a incidentelor în sistemul informatic. Administratorul de reţea autorizat să trateze solicitarea accesează staţia de lucru la nivel de "administrator" folosind parola adecvată, generează o nouă parolă de acces pentru utilizator şi o comunică pe loc acestuia. Accesul la staţia de lucru se face numai în prezenţa şi cu acordul utilizatorului staţiei de lucru. Imediat ce i-a fost comunicată, utilizatorul schimbă parola, urmând instrucţiunile pentru crearea şi modificarea parolei, astfel încât să o cunoască numai el. Parola creată de utilizator trebuie să respecte Regulile pentru stabilirea şi utilizarea parolei.

ART. 10

Ori de câte ori se părăseşte staţia de lucru se închide sesiunea de lucru (aplicaţia) prin comanda "Log off" şi se blochează accesul la staţie prin combinaţia de taste CTRL+ALT+DEL şi butonul Lock sau combinaţia 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 opţiunea "On resume, password protect", stabilind un timp de aşteptare până la pornirea automată a screen saverului de 3-10 minute prin completarea câmpului "wait minutes" şi punând-o în funcţiune cu comanda "Apply".

CAP. III

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

ART. 12

Sistemul de management al identităţii <Mgmtld> este un nou sistem informatic, care este în curs de implementare şi urmează a fi generalizat la nivelulMFP şi al instituţiilor subordonate. Are ca scop administrarea în mod centralizat a accesului la toate aplicaţiile informatice şi posturile de lucru, folosind identificarea sigură a persoanei şi un ansamblu de roluri stabilite de personalul îndreptăţit.

ART. 13

Accesul la staţiile de lucru se face diferenţiat, după cum utilizatorul staţiei respective face parte sau nu din Active Directory <AD> (platforma software dedicată administrării staţiilor de lucru care interacţionează cu funcţiile de administrare a conturilor utilizatorilor sistemelor de operare Windows) astfel:

a) cazul staţiilor ai căror utilizatori sunt integraţi în <AD>:

(i) sistemul de management al identităţii <Mgmtld> generează o parolă iniţială (default) pentru userul în cauză;

(ii) Active Directory la rândul său, prin politicile stabilite de către administratorul serverului de Domain Controller, obligă utilizatorul să îşi schimbe parola la prima logare;

(iii) în caz de pierdere a parolei, userul este obligat să apeleze la punctul de contact Help desk şi 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 şi forţând utilizatorul (automat, prin politicile stabilite în <AD>) să o modifice la primul "Log on";

b) cazul staţiilor ai căror utilizatori nu sunt integraţi în <AD>:

(i) sistemul de management al identităţii <Mgmtld> generează o parolă de acces iniţială pentru utilizatorul în cauză, dar nu îl forţează, prin politicile sale, să îşi schimbe parola la prima logare;

(ii) utilizatorul trebuie să respecte normele interne prezente şi să procedeze la schimbarea parolei iniţiale cu o parolă personală, setată la următorul "Log on";

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

ART. 14

Schimbarea parolei se face de către utilizator imediat după primirea/preluarea staţiei de lucru (la primul "Log on"), astfel încât să o cunoască numai el, conform Regulilor de stabilire şi 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 şi 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 anunţe despre acest eveniment conducerea direcţiei. Evenimentul trebuie să fie consemnat de către secretara direcţiei în Jurnalul de evidenţă a incidentelor de acces la sistemul informatic întreţinut în cadrul direcţiei. Schimbarea se face de către utilizator în conformitate cu Regulile pentru stabilirea şi 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 decontact Help desk.

ART. 17

Schimbarea parolei se face de către utilizator dacă a depăşit numărul maxim de încercări nereuşite de înscriere a parolei (a uitat parola). Utilizatorul trebuie să anunţe despre acest eveniment conducerea direcţiei. Evenimentul trebuie să fie consemnat de către secretara direcţiei în Jurnalul de evidenţă a incidentelor de acces la sistemul informatic întreţinut în cadrul direcţiei, apoi utilizatorul trebuie să apeleze la suportul tehnic furnizat de punctul de contact Help desk.

ART. 18

Solicitarea de asistenţă pentru schimbarea parolei este consemnată de personalul punctului de contact Help desk în Jurnalul de evidenţă a incidentelor în sistemul informatic. Persoana care tratează solicitarea contactează telefonic secretariatul direcţiei în care este încadrat solicitantul şi verifică identitatea solicitantului, precum şi dacă evenimentul a fost consemnat în Jurnalul de evidenţă a incidentelor de acces la sistemul informatic întreţinut în cadrul direcţiei.

ART. 19

Dacă solicitarea de schimbare a parolei nu este îndreptăţită, adică utilizatorul nu este salariat în cadrul direcţiei sau evenimentul nu este consemnat în Jurnalul de evidenţă a incidentelor de acces la sistemul informatic întreţinut în cadrul direcţiei, persoana care tratează solicitarea consemnează despre aceasta în Jurnalul de evidenţă a incidentelor în sistemul informatic, comunică despre aceasta prin poştă electronică internă secretarei direcţiei, solicitând consemnarea evenimentului şi în Jurnalul de evidenţă a incidentelor de acces la sistemul informatic întreţinut în cadrul direcţiei. Dacă solicitarea de schimbare a parolei nu este îndreptăţită, nu se va genera o nouă parolă.

ART. 20

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

ART. 22

Schimbarea parolei pe staţia de lucru se face de către utilizatorul final prin tastarea combinaţiei de taste CTRL+ALT+DEL şi butonul "Change Password".

ART. 23

Ori de câte ori se părăseşte staţia de lucru se închide sesiunea de lucru (aplicaţia) prin comanda "Log off" şi se blochează accesul la staţie prin combinaţia de taste CTRL+ALT+DEL şi butonul "Lock" sau combinaţia 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 opţiunea "On resume, password protect", stabilind un timp de aşteptare până la pornirea automată a screen saverului de 3-10 minute prin completarea câmpului "wait minutes" şi punând-o în funcţiune cu comanda "Apply".
