Anexa

AGENŢIA NAŢIONALĂ DE ADMINISTRARE FISCALĂ

Nr. ...../ .....20...

CONSILIUL JUDEŢEAN

Nr. ..222...../ .29.10.2015

PROTOCOL DE COLABORARE

În temeiul următoarelor prevederi legale:

Legea administraţiei publice locale nr.215/2001, republicată, cu modificările şi completările ulterioare,

Dispoziţiile **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,

Prevederile **art. 11, art.60, 61 şi 62 din Ordonanţa Guvernului nr. 92/2003 privind Codul de procedură fiscală**, republicată cu modificările şi completările ulterioare,

Prevederile **art. 7, litera A, pct. 23 din Hotărârea Guvernului nr. 520/2013** privind organizarea şi funcţionarea Agenţiei Naţionale de Administrare Fiscală, cu modificările şi completările ulterioare,

Prevederile **Ordinului ministrului finanţelor publice nr.2875/13.10.2009** pentru aprobarea instrucţiunilor privind utilizarea sistemului informatic din cadrul Ministerului Finanţelor Publice,

Prevederile **Ordinului ministrului finanţelor publice nr.551/24.04.2003** pentru aprobarea Instrucţiunilor de aplicare a prevederilor titlului - "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,

Prevederile **Legii nr. 455/2001 privind semnătura electronică, republicată,**

Prevederile **Hotărârii Guvernului nr.1259/2001 privind aprobarea Normelor tehnice şi metodologice** pentru aplicarea Legii nr. 455/2001 privind semnătura electronică,

Prevederile **Ordinului comun M.A.I.nr.279/M.F.P.nr.1736/2012** privind aprobarea modelului cadru al protocolului de cooperare în vederea schimbului de informaţii între Agenţia Naţională de Administrare Fiscală şi autorităţile administraţiei publice locale, publicat în Monitorul Oficial nr. 32/15.01.2013,

Prevederile **art. 2.3 paragraful 6 din Protocolul de colaborare dintre ANAF şi MSI** înregistrat cu nr. ANAF/A_PRS1873/23.06.2015 şi MSI/1837/23.06.2015.

Agenţia Naţională de Administrare Fiscală prin Administratia Finanțelor Publice Județene, cu sediul ....., reprezentată prin domnul ....., în calitate de șef administrație,

şi

Consiliul Județean, 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 scopul:

a) creşterii nivelului de colectare taxelor şi impozitelor la bugetul general consolidat al statului;
b) prevenirii şi combaterii evaziunii fiscale;
c) implementării şi atingerii obiectivelor proiectelor finanțate în cadrul operațiunii 3.2.1. **„Susţinerea implementării de soluţii de e-guvernare şi asigurarea conexiunii la broadband, acolo unde este necesar".**

Art. 2. Obligaţiile părţilor

În termen de maxim 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 Consiliilor Judeţene:

2.1.1. Consiliul Judeţean va transmite ANAF datele înregistrate în Registrul Agricol Electronic .

2.1.2. Consiliul Judeţean

a) va respecta prevederile legale referitoare la protecţia datelor personale şi a informaţiilor fiscale, prin utilizarea informaţiilor furnizate de către ANAF numai în scopurile prevăzute de lege;
b) va respecta procedura şi normele de conectare la reţea şi la serviciile oferite de sistemul informatic al Ministerului Finanţelor Publice, stabilite de către ANAF şi Serviciul de Telecomunicaţii Speciale;
c) va asigura cunoaşterea şi respectarea de către personalul desemnat al consiliului judeţean a prevederilor Ordinului ministrului finanţelor publice nr. 2875/13.10.2009 privind utilizarea sistemului informatic din cadrul Ministerul Finanţelor Publice (**anexa nr.1** la protocol), inclusiv însuşirea şi respectarea prevederile referitoare la utilizarea suporturilor (externe) de certificate digitale;
d) va colabora cu Serviciul de Telecomunicaţii Speciale în vederea asigurării canalului securizat pentru accesul personalului desemnat al consiliilor judeţene, la Sistemul Informatic al Ministerului Finanţelor Publice.

2.2. Obligaţiile Agenţiei Naţionale de Administrare Fiscală

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 Consiliului judeţean numai în scopurile prevăzute de lege.

2.2.2. ANAF va asigura accesul la informaţii, în forma dematerializată, personalului Consiliului judeţean desemnat în acest scop, în cadrul serviciului oferit de sistemul informatic al Ministerului Finanţelor Publice, la informaţiile prevăzute în anexa tehnică la Protocolul dintre ANAF şi MSI înregistrat cu nr. ANAF/A_PRS1873/23.06.2015 şi MSI/1837/23.06.2015.

2.2.3. Direcţia Generală a Tehnologiei Informaţiei din cadrul Agenţiei Naţionale de Administrare Fiscală :

a) asigură personalului consiliul judeţean 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;
b) colaborează cu Serviciul de Telecomunicaţii Speciale în vederea asigurării accesului securizat al personalului desemnat al consiliul judeţean, la Sistemul Informatic al Ministerului Finanţelor Publice.

Art.3. Modalităţi de realizare a schimbului de informaţii

3.1. Schimbul de informaţii între părţi se va realiza cu respectarea legislaţiei în vigoare, conform procedurii de lucru comună.

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, 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, cât şi pentru perfecţionarea cooperării.

4.3. Nerespectarea obligaţiilor asumate prin prezentul Protocol de către una dintre părţi dă dreptul parţii lezate de a cere rezilierea prezentului Protocol, cu o notificare prealabilă din parte acesteia cu minim 15 zile înainte.

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. Anexa nr. 1 la protocol face parte integrantă din acesta.

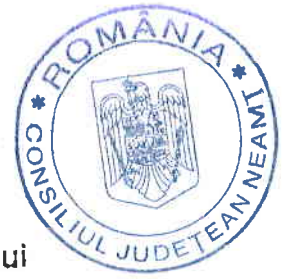
4.7. Prezentul Protocol intră în vigoare de la data semnării de către ultima parte.

4.8. Prezentul Protocol este valabil pe o perioada 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	**CONSILIUL JUDEŢEAN**
p. PREŞEDINTE	**REPREZENTANT**
Sef administraţie	

ANEXA Nr. 1 la
PROTOCOLUL DE COLABORARE



ORDIN nr. 2873/____
pentru aprobarea instrucțiunilor privind utilizarea sistemului informatic din cadrul Ministerului Finanțelor Publice

Ministrul Finanțelor Publice,

În temeiul art. 10 alin.(4) din Hotărârea Guvernului nr. 34/2009 privind organizarea şi funcționarea Ministerului Finanțelor Publice

emite prezentul ordin:

Art. 1. Se aprobă Instrucțiunile privind utilizarea sistemului informatic din cadrul Ministerului Finanțelor Publice, prevăzute în Anexa care face parte integrantă din prezentul ordin.

Art. 2. Responsabilitatea aplicării prezentului ordin revine tuturor salariaților din cadrul aparatului central al Ministerului Finanțelor Publice şi din instituțiile publice subordonate, funcționari publici sau personal contractual.

Art. 3. Compartimentele aparatului central al Ministerului Finanțelor Publice şi din instituțiile publice subordonate pot elabora norme proprii mai stricte pentru utilizarea sistemului în conformitate cu aceste instrucțiuni şi cu procedurile proprii.

Bucureşti: 13.10.2009

MINISTRUL FINANȚELOR PUBLICE,
Gheorghe POGEA
9.10.2009

ANEXĂ

Instrucțiunile 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, şi stabilesc reguli privind protejarea sistemului informatic al ministerului, conform legislației române în vigoare, precum şi Convențiilor Internaționale şi Reglementarilor 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 şi software şi 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 tastatura la stația de lucru;
c) *dispozitiv wireless*: echipament de tehnică de calcul şi 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 disc, modemurile;
e) *fişier multimedia*: fişier având o organizare internă dedicată stocării unei combinații de formate text, audio, fotografie, animație, film şi 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 utilizator (user name)*: cod alfanumeric atribuit persoanei ce urmează să acceseze resurse ale sistemului informatic;
h) *parola de acces (password)*: cod (şir 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 (servere, 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 și compartimentele din instituțiile publice subordonate aflate în coordonarea sa metodologică, denumită în continuare DGTI;
n) *rețea de date/ rețea de comunicații de date*: subansamblu al sistemului informatic format din patch cord-uri, prize de rețea, cablaj structurat, echipamente de comunicații, protocoale de comunicații și software pentru administrarea comunicațiilor. Rețeaua de date are roiul de a oferi suport hardware și software pentru interconectarea stațiilor lucru, serverelor, imprimantelor, etc. și pentru acces la serviciile informatice, inclusiv la poștă 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, transmitere și extragerea datelor pe cale electronică constituit în scopul oferirii de servicii informatice;

r) *stație de lucru*: ansamblul format din calculator şi echipamentele periferice destinat realizării sarcinilor de serviciu, conectat sau nu la rețeaua de date a MFP şi 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*: sursa neîntreruptibilă de tensiune; asigură alimentarea cu energie electrică a consumatorilor, un timp limitat, în cazul lipsei tensiunii în rețeaua publică;
u) *utilizatorul final/responsabil stație de lucru*: persoana angajată sau numită într-o funcție publică în cadrul MFP, care a primit dreptul de acces la stația de lucru şi drepturi de utilizare a resurselor sistemului informatic.

CAPITOLUL II
REGULI DE UTILIZARE A STAȚIEI DE LUCRU

Secțiunea 1: Întreținerea şi 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.

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, este marcat numele instituției şi numărul de inventar şi să păstreze copia fişei de inventar a stației de lucru precum şi a celorlalte echipamente de calcul aflate in inventarul său;
b) să amplaseze stația astfel încât să poată fi utilizată cu uşurință şi totodată ferită de lovirea accidentală, de şocuri şi vibrații, ferită de acțiunea directă a razelor solare, ferită de praf, fum, ploaie şi umezeală;
c) să pozeze cablurile astfel încât să nu împiedice circulația personalului;
d) să poziționeze stația în aşa 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 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 sau 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 pe 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 funcţionarea 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 distrugă etichetele aplicate pe echipamente;
q) să sprijine personalul abilitat pentru remedierea defecţiunilor furnizând informaţiile 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 apropie stația de surse de încălzire la o distanță mai mică de 1m;
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 corosive, toxice sau inflamabile;
i) să utilizeze stația cu mâinile ude sau murdare;
j) să lovească stația sau să o supună șocurilor sau vibrațiilor;
k) să depoziteze obiecte pe echipamente sau 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 a 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"* la prezentele instrucțiuni.

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, sau 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 regulile 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 utilizator (user name) și o parola de acces (password), care vor fi cunoscute numai de responsabilul stației.

Art. 19. Responsabilul de stație 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 şi la aplicațiile informatice centralizate în Intranetul MFP"*, prevăzută în *Anexa nr. 2* la prezentele instrucțiuni.

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 (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 afişa parola de acces prin scriere/tipărire pe hârtie sau post-it sau alte asemenea suporturi ;

b) nu va transmite parola de acces la alte persoane, inclusiv colegilor de birou chiar dacă aceştia se oferă să-l ajute în utilizarea stației de lucru;

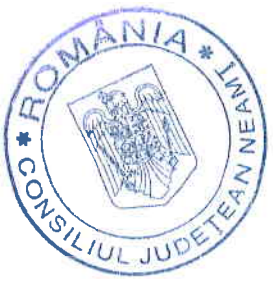
c) înainte de plecarea din sediu pentru perioade mai mari de timp (delegații, concedii, etc.) va pune la dispoziția colegilor săi datele care le-ar putea fi necesare pentru buna desfăşurare a activității, astfel încât aceştia să nu aibă nevoie ulterior de parola sa de acces;

d) dacă trebuie să lucreze pe o altă stație decât cea pentru care este responsabil, el va folosi propriul nume utilizator (user name) şi 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) utilizatorul final este singurul răspunzător de confidențialitatea parolei de acces, aceasta fiind mijlocul de autentificare şi 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 al stației de lucru, precum și modul de utilizare al 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 nici o 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 va 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 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 sistemul 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 sau ale parametrilor sistemelor pot 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 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 sa oprească sau să dezinstaleze programul de protecție 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 protecție antivirus este oprit.

Art. 38. În cazul în care foloseşte programe fără înştiințarea şi aprobarea DGTI, utilizatorul este direct răspunzător de efectele produse de încălcarea *Legii nr.8/1996 privind drepturile de autor şi drepturile conexe, cu modificările şi completările ulterioare.*

Art. 39. Numai proprietarul drepturilor asupra informațiilor poate autoriza ieşirea datelor din birou sau din sediu sau transmiterea datelor înafara 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 şi apoi să şteargă 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, şefului 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 dupa caz:
a) distrugerea fizică organizată: distrugerea controlată a hard-disk-urilor, a

suporturilor de stocare de date;
b) autorizarea reutilizării stațiilor de lucru după un control prealabil:ştergerea sigură a configurațiilor, ştergerea sigură a datelor prin rescrierea repetată a suportului.

CAPITOLUL III
ALTE DISPOZIȚII

Secțiunea 1: Reguli pentru stocarea şi 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 şi al compartimentului (direcției) care le foloseşte.

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

Art. 45. Depozitarea suporturilor trebuie făcută în locuri şi în condiții care să respecte indicațiile furnizorilor suporților respectivi şi o securitate fizică corespunzătoare.

Art. 46. Suporturile trebuie şterse înainte de a fi oferite spre reutilizare. Ştergerea trebuie sa 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 suporturile externe de stocare a datelor pentru copierea de fişiere, programe, date obținute din surse nesigure (din afara sistemului informatic al MFP, InterNet, prieteni, cunoscuți, etc.), pe stația de lucru, fără a fi verificați în prealabil cu programul de antivirus instalat pe aceasta.

Art. 48. Transportul suporturilor se asigură numai de persoane autorizate. Suporturile continând 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 şi citirea sau copierea de către persoane neautorizate.

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 şi/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 şi orice alt incident privind stația de lucru sau suporturile externe de stocare a datelor trebuie comunicat imediat conducerii compartimentului (direcției) 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 funcție de problemele ivite în funcționarea sistemelor sau serviciilor, remedierile 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 şi poate atrage după sine 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 şi orice mesaj care apare pe ecran;

b) trebuie izolat calculatorul față de rețea prin deconectarea patch cord-ului 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 şi/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 pierderea sau distrugerea informației în timpul sau în afara orelor de lucru normale.

Art. 57. Această politica trebuie să țină seama de clasificările de securitate a 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 poșta 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 de la Capitolul II privind utilizarea stației de lucru precum și dispozițiile Capitolului 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 este marcat numele instituției și numărul de inventar și să păstreze copia fișei de inventar a echipamentului;

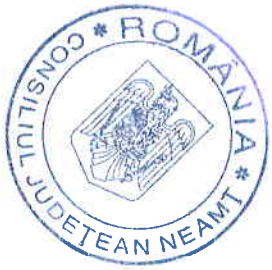
c) să cripteze datele folosind utilitarul instalat;
d) să salveze datele pe medii externe de stocare a informațiilor sau pe serverele de fișiere şi apoi să şteargă aceste date de pe echipament de îndată ce acestea şi-au îndeplinit scopul de utilizare;
e) să se asigure că ecranul stației mobile este setat 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 şi înainte de reconectarea acestuia în rețeaua de date a MFP să lanseze programul complet de devirusare instalat.

Art. 62. Responsabilul stației mobile trebuie să protejeze echipamentul, următoarele activități fiind interzise:
a) să lase echipamentul nesupravegheat sau să-l predea spre utilizare membrilor familiei, unor rude, prieteni, cunoscuți 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 siguranță ale aplicațiilor, datelor, programelor, etc. în acelaşi loc cu echipamentul (ex.: în geanta de protecție a echipamentului).

Secțiunea a 6-a: Măsuri disciplinare

Art. 63. (1) Încălcarea prezentelor instrucțiuni constituie abatere disciplinară şi atrage răspunderea disciplinară, potrivit legii.
(2) Măsurile disciplinare pot include şi interzicerea accesului la resursele sistemului informatic.

Art. 64. Anexele nr. 1 şi 2 fac parte integrantă din prezentele instrucțiuni.



Anexa nr.1 la Instrucțiuni

Securitatea sistemelor informatice

Procedurile de securitate ale sistemelor informatice se referă la securitatea fizică, hardware, software, de comunicații şi la securitatea datelor şi 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 fişă de inventar, salariaților din MFP;
b) uşile sunt încuiate la sfârşitul fiecărei zile şi numai personalul autorizat are acces la echipamentele de tehnologia informației şi comunicațiilor;
c) stațiile de lucru mobile sunt încuiate în dulapuri la sfârşitul fiecărei zile şi numai personalul autorizat are acces la aceste echipamente;
d) serverele funcționează în camere tehnice special amenajate în zone protejate şi 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 asigurata 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
i) calitate de vizitatori;
j) administratorul de rețea înregistrează toți vizitatorii la server, iar informațiile despre vizitatori sunt păstrate cel puțin doi ani;
k) conform *Legii nr. 349/2002, pentru prevenirea şi combaterea efectelor consumului produselor din tutun, cu modificările şi 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 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 decât 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, al 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 utilitarelor anti-virus;
d) utilizatorul este responsabil de utilizarea software-ului instalat;
e) utilizatorul le este interzisă modificarea configurării stației de lucru, sistemului de operare, rețelei și ai 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, este controlată şi blocată prin politicile serverului de Domain Controller;
h) utilizatorii trebuie sa respecte termenii licenţelor referitoare la drepturile de autor, precum şi prevederile Legii nr. 8/1996 privind dreptul de autor şi drepturile conexe; responsabilitatea în cazul încălcării acestei obligaţii revine utilizatorilor în cauză;
i) utilizatorilor finali le este interzisă îndepărtarea protecţiei anti-virus sau a oricăror alte aplicaţii; numai administratorul de reţea are această atribuţie;
j) pentru protecţia sistemului de 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-mail-urilor, salariaţii MFP îşi asumă personal responsabilitatea conţinutului respectiv, iar orice opinie sau afirmaţie în numele ministrului finanţelor publice, al ministerului sau al oricărei alte 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 reţelele 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 vulger, injurios, defăimător sau pentru a hărţui persoane;

i) securitatea conturilor de e-mail pe stații este asigurată de aplicații anti-virus;
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 a fi autorizat în acest sens;
m) este interzis a se face achiziții on-line fără a fi autorizat 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 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 improprii 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.*

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 al circulației informațiilor la nivel de rețea/servere 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, modifice, copieze sau să distrugă direct sau 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 asupra momentului exact când aceasta s-a întâmplat și nu va divulga sau propaga aceste informații;

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.*

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 nr. 2 la Instrucțiuni

**Procedura pentru asigurarea accesului autorizat
la stațiile de lucru şi la aplicațiile informatice centralizate
în Intranetul Ministerului Finanțelor Publice**

CAPITOLUL I
DISPOZIȚII GENERALE

Art. 1. Prezenta procedură este stabilită în conformitate cu Politica MFP privind asigurarea securității sistemului informatic, de telecomunicații şi de protecție a datelor şi 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 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 minim 1 majusculă, minim 1 cifră şi nici un caracter special (adică de tip .,:;?!@#$%&*<>-_+=);
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 nereuşite de înscriere a parolei este 5;
h) durata blocării accesului după depăşirea numărul maxim de încercări nereuşite de înscriere a parolei: 30 minute;
i) parola nu se comunică nici unei alte persoane;
j) utilizatorul răspunde de utilizarea parolei.

CAPITOLUL II
Procedura aplicată în cazul personalului care nu utilizează Sistemul de management al identității <MgmtId>

Art. 3. Pentru salariații care nu utilizează sistemul de management al identității <MgmtId> 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 <MgmtId> va fi pus în funcțiune, numărul utilizatorilor procedurii se va restrânge.

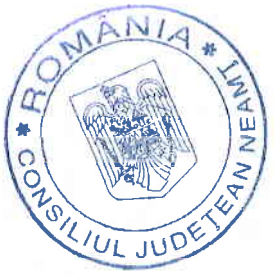
Art. 4. Contul utilizatorului pe stația de lucru este un cod alfanumeric şi este stabilit de către administratorul de rețea şi este public.

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 de stabilire şi utilizare a parolei şi urmând instrucțiunile 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 anunțe despre acest eveniment conducerea direcției. Evenimentul trebuie să fie consemnat de către secretara direcției în *Jurnalul de evidență al incidentelor de acces la sistemul informatic întreținut în cadrul direcției.* Schimbarea se face de către utilizator în conformitate cu *Regulile pentru stabilirea şi utilizarea parolei şi urmând instrucțiunile pentru crearea şi modificarea parolei.*

Art. 8. Schimbarea parolei se face, de asemenea, de către utilizator dacă a depăşit numărul maxim de încercări nereuşite 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 al 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 şi o comunică pe loc acestuia. Accesul la stația de lucru se face numai în prezența şi cu acordul utilizatorului stației de lucru. Imediat ce i-a fost comunicată, utilizatorul schimbă parola, urmând instrucțiunile 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 stația de lucru se închide sesiunea de lucru (aplicația) prin comanda "Log off" şi se blochează accesul la stație prin combinația de taste CTRL+ALT+DEL şi 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 aşteptare până la pornirea automată a screen saver-ului de 3-10 minute prin completarea câmpului wait minutes şi punându-o în funcțiune cu comanda Apply.

CAPITOLUL III
Procedura aplicată în cazul personalului care utilizează Sistemul de Management al Identității <MgmtId>

Art. 12. Sistemul de management al identității <MgmtId> este un nou sistem informatic, care este în curs de implementare şi urmează a fi generalizat la nivelul MFP şi al instituțiilor subordonate. Are ca scop administrarea în mod centralizat a accesului la toate aplicațiile informatice şi posturile de lucru, folosind identificarea sigură a persoanei şi 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 <MgmtId>, generează o parola inițială, (default), pentru userul în cauză;

ii. Active Directory la rândul sau, prin politicile stabilite de către administratorului serverului de Domain Controller, obligă utilizatorul să-şi 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 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 <MgmtId>, generează o parolă de acces inițială, pentru utilizatorul în cauză, dar nu-l forțează, prin politicile sale, să-şi schimbe parola la prima logare;

ii. Utilizatorul trebuie să respecte normele interne prezente şi 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 <MgmtId>va fi extins şi generalizat.

Art. 14. Schimbarea parolei se face de către utilizator imediat după primire, preluarea stației 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 anunțe despre acest eveniment conducerea direcției. Evenimentul trebuie să fie consemnat de către secretara direcției în *Jurnalul de evidență al incidentelor de acces la sistemul informatic* întreținut în cadrul direcției. 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 de contact 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 anunțe despre acest eveniment conducerea direcției. Evenimentul trebuie să fie consemnat de către secretara direcției în *Jurnalul de evidență al 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 şi verifică identitatea solicitantului precum şi dacă evenimentul a fost consemnat în *Jurnalul de evidență al 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 era consemnat în *Jurnalul de evidență al 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 poştă electronică internă secretarei direcției, solicitând consemnarea evenimentului şi în *Jurnalul de evidență al 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*, generează imediat o nouă parolă de acces şi o comunică imediat 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 stația de lucru se face de către utilizatorul final prin tastarea combinației de taste CTRL+ALT+DEL şi butonul Change Password.

Art. 23. Ori de câte ori se părăseşte stația de lucru se închide sesiunea de lucru (aplicația) prin comanda "Log off" şi se blochează accesul la stație prin combinația de taste CTRL+ALT+DEL şi 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 aşteptare până la pornirea automată a screen saver-ului de 3-10 minute prin completarea câmpului wait minutes şi punându-o în funcțiune cu comanda Apply.