Anexa nr. 9
la Caietul de sarcini

LUKOIL OIL COMPANY

S.C. PETROTEL-LUKOIL S.A.

DAB 0182-28.04.11

D E C I Z I E

Privind aprobarea Politicii şi a
Cerinţelor pentru asigurarea securitatii
informaţionale

Având în vedere necesitatea îmbunătăţirii măsurilor de asigurare a securitatii informationale la exploatarea echipamentelor informatice din intreprindere,
DECID:

1. Se aprobă Politica securităţii informaţionale (Anexa 1) şi Cerinţele de asigurare a securităţii informaţionale la exploatarea ulterioară a echipamentelor informatice (Anexa 2) (în continuare Politica şi Cerinţe).

2. Directorii Generali Adjuncţi, şefii compartimentelor structurale şi specialiştii principali vor aduce la cunoştinţa angajaţilor Politica şi Cerinţele şi până la 31.05.2011 vor prezenta Serviciului Control Intern şi Protecţie listele persoanelor care au luat la cunostinţă.

3. Directorul General Adjunct Personal şi Probleme Generale va asigura, în termen de o lună de la data angajării, aducerea la cunoştinţă a noilor angajaţi cu Politica şi Cerinţele.

4. Controlul executarii prezentei decizii ii revine I. Besciotnii - Sef Serviciu Control Intern si Protectie.

Director General

S.C. PETROTEL-LUKOIL S.A. PLOIEŞTI, ROMANIA
SEMNAT
D-SISTEM

I. Kuzmin

Besciotnii
3311

DAB 0182-28.04.11

Anexa 1
la Decizia nr.___din _____

POLITICA SECURITATII INFORMATIONALE[1] "PETROTEL-LUKOIL"

1.1. UTILIZAREA PAROLELOR

Scopul si domeniul aplicarii

«Politica securitatii informationale "PETROTEL-LUKOIL" Utilizarea parolelor» (in continuare – Politica) stabileste regulile de baza privind utilizarea parolelor pentru accesul la activele informationale "PETROTEL-LUKOIL" (in continuare – Societatea), sau a activelor informationale, aflate in deservirea Companiei.

Politica va fi aplicata in mod obligatoriu de catre toti angajatii Societatii si persoanele terte care utilizeaza activele informationale ale acesteia.

Cerintele prezentei Politici vor fi respectate in masura posibilitatilor tehnice ale activului.

Prevederile politicii

Accesul la activele informationale ale Societatii sau a clientilor se realizeaza prin utilizarea inregistrarilor personale de evidenta si parolelor din cifre si litere care vor fi modificate periodic, tinand cont de urmatoarele cerinte:

- parola contine nu mai putin de opt simboluri, incluzind litere din ambele registre si cifre;
- parola nu trebuie sa fie un cuvant care se gaseste in dictionare sau termen de specialitate, inclusiv scris folosind o alta dispunere a tastelor;
- parola nu trebuie sa contina informatii usor accesibile legate de familie, serviciu (nume, prenume, data de nastere, numele animalelor, numerele auto sau de telefon, denumirea organizatiilor, adrese electronice etc.);
- parola nu trebuie sa contina o succesiune de numere usor de descoperit (123456, aaabbb, qwerty, q1w2e3 etc.).

Una din metodele de creare a parolelor sigure si usor de memorat este codificarea unui vers sau expresii. De exemplu parola creata pe baza frazei (in rusa): "Iata un exemplu de parola sigura si usor de memorat" este (poate fi): "Vot1PN&ZP" (in romana – Iata1EP&UM).

Parola provizorie creata de administrator in cazul inregistrarilor de evidenta sau modificarii parolei uitate trebuie sa fie unica si sa fie transmisa excluzand posibilitatea accesului altor persoane si va fi modificata de catre utilizator in cazul primei accesari a activului.

Parolele prestabilite de catre producator vor fi modificate inainte de exploatarea activului.

Parolele inregistrarilor de evidenta cheie aferente activelor informationale critice vor fi pastrate intr-un plic in seiful conducatorului compartimentului – detinatorului activului respectiv.

Parolele vor fi clasificate ca Secret de Serviciu si se vor pastra conform Normelor de Protectie a Informatiilor Clasificate

SE INTERZICE:

[1] Prin Securitatea Informationala in prezentul document se inteleg actiuni cu caracter organizational si tehnic cu privire la securitatea informatiei de la acces neautorizat al tertilor

- sa se comunice altor persoane parola personala sau scrierea acesteia pe un suport material accesibil altor persoane (in afara cazurilor cand este prevazuta pastrarea parolelor inregistrarilor cheie de catre detinatorul activului);
- pastrarea parolelor cand mijloacele tehnice sunt in functiune sau folosirea mijloacelor de introducere automata;
- utilizarea unui algoritm de modificare a parolei usor de descoperit (de exemplu, F%1hTR8→ F%2hTR8→ F%3hTR8, sau F%1hTR8→ F1%hTR8→ F1h%TR8 etc.)
- utilizarea inregistrarilor de evidenta ale altor persoane;
- utilizarea in afara Societatii a parolelor care coincid cu parolele de acces la activele informationale a acesteia;
- utilizarea in calitate de parola a exemplelor din prezentul document.

Parola se va modifica o data la 6 luni sau in cazul depistarii situatiilor de compromitere, iar in ccea ce priveste inregistrarile de evidenta administrativa – odata cu schimbarea persoanei care indeplineste functiile de administrator.

Parolele se vor intocmi de «PETROTEL-LUKOIL» si vor fi avizate de S.C.I.P.

In functie de caracterul critic al activului tehnico-informational detinatorul poate stabili cereri mai ridicate fata de complexitatea parolei si periodicitatea modificarii acesteia.

Procesele de creare, modificare, utilizare, blocare, anularea inregistrarilor de evidenta, precum si de modificare a parolelor vor fi reglementate, cu conditia exercitarii controlului asupra acestor procese si intocmirea de procese-verbale.

Rolul si obligatiile

Obligatia privind respectarea prevederilor prezentei Politici este in sarcina tuturor angajatilor Societatii si persoanelor terte care utilizeaza activele tehnico-informationale, activele informationale care se afla in deservirea Companiei a acesteia.

Toate derogarile de la politica vor fi avizate de catre Departamentul tehnologiei informationale, S.C.I.P. si deasemenea cu departamentele raspunzatoare de protectia informatiei clientilor care transfera activele informationale in deservirea Societatii de la acces nepermis, iar derogarile neavizate vor fi considerate incidente si pot servi ca baza pentru sanctionarea pentru derogarea de la politica stabilita conform legislatiei Romaniei sau clauzelor conventiei dintre parti.

Controlul privind indeplinirea Politicii si reanalizarea conditiilor revin Departamentului tehnologiei informationale a «PETROTEL-LUKOIL» si a companiilor din grupul Lukoil.

Dupa efectuarea controlului, «PETROTEL-LUKOIL» va intocmi un Raport privind incalcarile constatate, Raportul va fi prezentat S.C.I.P. pentru luare la cunostinta si avizarea acestuia, ulterior va fi prezentat conducerii companiei.

1.2. GESTIONAREA ACCESULUI

Scopul si domeniul aplicarii

"Politica securitatii informationale «PETROTEL-LUKOIL» Gestionarea accesului" (in continuare - Politica) stabileste regulile si cerintele de baza privind organizarea si controlul accesului angajatilor Societatii si tertilor (in continuare – Utilizatori) la activele tehnologice informationale care sustin procesele de business ale «PETROTEL-LUKOIL».

Din categoria activelor tehnologice informationale fac parte resursele informationale, aplicatiile de business, servicii (de exemplu, posta electronica, Internet, telefonie) si alte componente tehnologice ale infrastructurii informationale a Societatii.

Politica este valabila pentru angajatii Societatii care au calitatea de detinatori ai activelor tehnologice informationale sau care gestioneaza accesul la acestea si este obligatorie pentru indeplinire.

Prevederile politicii

Fiecare activ tehnologico-informational trebuie repartizat unui angajat din compartimentul din structura in obligatia caruia intra stabilirea si revizuirea regulilor de gestionare a accesului si controlul respectarii acestora.

Acordarea accesului la activul tehnologic informational se face in urma deciziei detinatorului acestuia conform procedurii stabilite de detinator si aprobata de Directia securitatii informationale si S.C.I.P. privind acordarea accesului, precum si de persoana care gestioneaza drepturile de acces ale utilizatorilor la activul tehnologic informational (in continuare – Administrator).

Accesul la activele tehnologice informationale trebuie acordat dupa efectuarea evaluarii riscurilor aferente conform cerintelor de business si a obligatiilor functionale ale utilizatorilor, daca este posibil conform grupei carecuprinde utilizatorii cu obligatii functionale adiacente.

Utilizarea accesului la activele tehnologice informationale trebuie controlata si intocmite protocoale, iar utilizatorii trebuie sa ia la cunostinta de raspunderea pe care o au in cazul utilizarii acestora in mod ilegal si sa respecte cerintele referitoare la protectia acestora stabilite de detinatorii activelor tehnologice informationale.

Drepturile de acces ale utilizatorilor trebuie analizate in mod regulat de catre detinatorii activelor tehnologice informationale pentru a evidentia drepturile depasite sau excedentare, iar accesul angajatilor Societatii concediati sau transferati si ai tertilor care si-au incheiat activitatea pe baza contractelor trebuie revizuit sau sistat.

Sistemele automatizate de gestionare a accesului trebuie sa contina mecanisme de gestionare prin inregistrarea datelor de evidenta si sa functioneze pe baza procedurii standard de autorizare a utilizatorului care foloseste datele inregistrate si parola.

Accesul la activele tehnologice informationale cu utilizarea datelor de inregistrare fara parola este interzis, iar utilizarea datelor de inregistrare cu drepturile de administrare si accesul la utilitatile de mijloacele de sistem de diagnosticare trebuie supuse unui control special din partea detinatorului activului tehnologic informational.

Softurile care sustin procesele de business critice trebuie grupate si separate in mod logic de celelalte (de exemplu, cu utilizarea ecranelor intraretele), iar conectarea mijloacelor soft care prelucreaza informatii strict confidentiale la retelele de telecomunicatii este interzisa.

La utilizarea accesului de la distanta sau fara fir trebuie sa se foloseasca mecanismele autentificarii intensificate, codificarii si verificarii configuratiei statiei automatizate de la distanta privind conformitatea cu cerintele de securitate.

Componenta, arhitectura si configuratia mijloacelor soft utilizate pentru gestionarea accesului trebuie sa fie standardizate, iar procesele instalarii acestora, setarii, activizarii, exploatarii si actualizarii trebuie reglementate, prevazute in protocoale si controlate.

Cine raspunde

Angajatii Societatii care indeplinesc functiile detinatorilor activelor tehnologice informationale sau realizeaza gestionarea accesului la acestea raspund de respectarea prevederilor Politicii.

Toate derogarile de la Politica trebuie sa fie convenite cu Directia securitatii informationale. Abaterile neautorizate de la prevederile Politicii se considera incidente in domeniul securitatii informationale si pot sta la baza tragerii la raspundere conform legislatiei Romaniei sau acordului dintre parti.

Controlul pentru indeplinirea politicii si actualizarea acesteia revine S.C.I.P al «PETROTEL-LUKOIL» si a companiilor din grupul Lukoil.

Rezultatele controlului vor fi prezentate de «PETROTEL-LUKOIL» pe baza de Raport S.C.I.P., pentru luarea la cunostinta si avizarea acestuia.

Supravegherea indeplinirii acestor Politici si a controalelor efectuate de «PETROTEL-LUKOIL» ii revine Serviciului Control Intern si Protectie.

1.3. UTILIZAREA POSTEI ELECTRONICE

Destinatia si domeniul de aplicare

"Politica securitatii informationale "PETROTEL-LUKOIL" privind utilizarea postei electronice" (in continuare - Politica) stabileste regulile si cerintele de baza de protectia activelor informationale si a reputatiei "PETROTEL-LUKOIL" (in continuare - Societate) impotriva amenintarilor legate de utilizarea postei electronice.

Politica este valabila pentru toti angajatii Societatii si tertii care utilizeaza mijloacele soft si hard ale Societatii pentru a primi sau transmite mesaje prin posta electronica si a carei implementare este obligatorie.

Prevederile politicii

Utilizarea postei electronice trebuie autorizata conform procedurii in vigoare referitoare la acordarea accesului la active informationale si se face prin adresele postale electronice in domeniul postal al Societatii.

Utilizarea postei electronice trebuie efectuata numai pentru indeplinirea sarcinilor functionale.

Informatiile confidentiale transmise prin utilizarea postei electronice trebuie sa fie protejate fata de vizualizarea neautorizata sau modificare. Se interzice transmiterea informatiilor strict confidentiale prin utilizarea postei electronice.

Se interzice utilizarea postei electronice care incalca normele legislatiei in vigoare, ale eticii si culturii corporative, precum si drepturile de autor si drepturile conexe ale altor persoane sau care reprezinta orice forma de urmarire a identitatii.

Actiunile de transmitere si primire a mesajelor de posta electronica trebuie inregistrate, iar mesajele trebuie salvate.

In mesajele e-mail transmise destinatarilor terti trebuie adaugata informatia care exonereaza Societatea de raspundere pentru continutul mesajului si care il previne pe destinatarul mesajului ca raspunde pentru utilizarea fara drept a mesajului.

Trebuie intreprinse masurile de prevenirea transmiterii mesajelor anonime nesolicitate, inclusiv a celor cu caracter publicitar (spam).

Inainte de transmiterea mesajelor pe e-mail trebuie verificata corectitudinea adreselor destinatarilor.

Societatea isi rezerva dreptul sa nu efectueze transmitera mesajului in cazul in care nu se respecta cerintele Politicii.

Continutul, architectura si configuratia serverelor de e-mail ale Societatii trebuie sa fie standardizate, iar procesele de instalare, setare, activare, exploatare si updatare a acestora trebuie sa fie reglamentate, controlate si inregistrate.

Functii si raspunderi

Raspunderea pentru respectarea Politicii revine tuturor angajatilor Societatii si tertilor care utilizeaza mijloacele soft si hard ale Societatii pentru transmiterea si primirea de e-mail.

Toate exceptiile din Politica trebuie sa fie convenite cu Departamentul tehnologiei informationale. Abaterile neautorizate de la prevederile Politicii se considera incidente de securitate informationala si pot saa la baza tragerii la raspundere conform legislatiei Romaniei sau acordului dintre parti.

Controlul privind indeplinirea Politicii si revizuirea acesteia revine Departamentului tehnologiei informationale a «PETROTEL-LUKOIL» si a companiilor din grupul Lukoil. Rezultatele controlului vor fi aduse la cunostinta S.C.I.P. de catre «PETROTEL-LUKOIL», sub forma de Raport care ulterior va fi avizat.

1.4. UTILIZAREA RETELEI INTERNET

Destinatia si domeniul de aplicare

"Politica securitatii informationale «PETROTEL-LUKOIL » privind utilizarea retelei internet" (in continuare - Politica) stabileste regulile si cerintele de baza de protectie a activelor informationale si a reputatiei «PETROTEL-LUKOIL» (in continuare - Societate) impotriva amenintarilor legate de utilizarea retelei Internet.

Politica este valabila pentru toti angajatii Societatii si tertii care utilizeaza mijloacele soft si hard ale Societatii pentru a accesa reteaua Internet si a carei aplicare este obligatorie.

Prevederile politicii

Accesul la reteaua Internet trebuie autorizat conform procedurii in vigoare referitoare la acordarea accesului la active informationale.

Accesarea retelei Internet trebuie efectuata numai pentru indeplinirea sarcinilor functionale.

Informatiile confidentiale transmise prin utilizarea retelei Internet trebuie sa fie protejate fata de vizualizarea neautorizata sau modificare. Se interzice transmiterea informatiilor strict confidentiale prin utilizarea retelei Internet.

Se interzice utilizarea retelei Internet care incalca normele legislatiei in vigoare, ale eticii si culturii corporative, precum si drepturile de autor si drepturile conexe ale altor persoane.

Se interzice utilizarea retelei Internet cu scopul publicarii informatiilor in numele Societatii fara aprobarea conducerii.

Continutul si volumul informatiilor transmise sau preluate prin utilizarea retelei Internet pot fi limitate.

Societatea isi rezerva dreptul sa monitorizeze utilizarea retelei Internet in scopul indeplinirii prevederilor Politicii.

Continutul, architectura si configuratia mijloacelor soft si hard folosite pentru preluarea sau transmiterea informatiilor prin reteaua Internet trebuie sa fie standardizate iar procesele de instalare, setare, activare, exploatare si updatare trebuie sa fie reglamentate, controlate si inregistrate.

Functii si raspunderi

Raspunderea pentru respectarea Politicii revine tuturor angajatilor Societatii si tertilor care utilizeaza mijloacele soft si hard ale Societatii pentru accesarea retelei Internet.

Toate exceptiile din Politica trebuie sa fie convenite cu Departamentul tehnologiei informationale. Abaterile neautorizate de la prevederile Politicii se considera incidente de securitate informationala si pot sta la baza tragerii la raspundere conform legislatiei Romaniei sau acordului dintre parti.

Controlul asupra indeplinirii Politicii si revizuirea acesteia revine Departamentului tehnologiei informationale a «PETROTEL-LUKOIL» si a companiilor din grupul Lukoil.

In dependenta de cele constatate «PETROTEL-LUKOIL» va prezenta informatia pe baza de Raport S.C.I.P., pentru luarea la cunostinta si avizarea acestuia.

1.5. INVENTARIEREA ACTIVELOR INFORMATIONALE

Scopul si domeniul aplicarii

"Politica securitatii informationale «PETROTEL-LUKOIL» Inventarierea activelor informationale" (in continuare – Politica) stabileste regulile si cerintele de baza privind identificarea si desemnarea persoanelor care vor raspunde de activele informationale critice ale «PETROTEL-LUKOIL» (in continuare – Societatea).

Politica va fi aplicata in mod obligatoriu de catre conducatorii compartimentelor din structura Societatii, angajatii din cadrul serviciilor care asigura securitatea informationala si angajatii desemnati de catre detinatorii activelor informationale.

Prevederile politicii

Inventarierea activelor informationale va fi realizata in cadrul compartimentelor Societatii inainte de darea in exploatare, precum si anual, conform metodicii unitare aprobate de catre Conducerea Societatii.

Vor fi identificate toate activele informationale importante pentru Societate din punct de vedere al daunelor provocate de incalcarea regulilor securitatii si va fi desemnata persoana din cadrul compartimentului care va indeplini functiile detinatorului.

Obligatiile detinatorului activului informational:

- prezentarea datelor necesare privind activul in scopul inregistrarii in Registrul activelor informationale, evaluarea riscurilor, planificarea continuitatii activitatii in conditii de disfunctii si catastrofe;
- clasificarea informatiilor, stabilirea si reanalizarea regulilor de administrare a accesului, precum si acordarea si sistarea dreptului de acces la activul informational;
- aplicarea in ceea ce priveste activul informational a masurilor de securitate prevazute in politicile, regulamentele si instructiunile Societatii privind asigurarea securitatii informationale, precum si in Planul de gestionare a riscurilor;
- stabilirea si controlul privind aplicarea cerintelor de securitate a activului informational de catre utilizatorii din cadrul Societatii si persoanele terte.

In cazul delegarii unei parti din obligatii de catre detinator (de exemplu, administrarea competentelor utilizatorilor, gestionarea mijloacelor tehnice de securitate) catre un compartiment specializat, aceasta se va consemna in Registrul activelor informationale, iar sarcina privind asigurarea securitatii activului informational ramane obligatia detinatorului respectiv.

Rolul si obligatiile

Obligatia privind inventarirea si completarea Registrului activelor informationale este in sarcina compartimentelor de securitate informationala.

Obligatia privind desemnarea detinatorilor activelor informationale si inlocuirea acestora in cazul schimbarilor de cadre este in sarcina conducatorilor compartimentelor din structura.

Obligatia privind securitatea activelor informationale este in sarcina detinatorilor.

Toate derogarile de la politica vor fi avizate de catre serviciul care raspunde de securitatea informationala, iar derogarile neavizate vor fi considerate incidente si pot servi ca baza pentru sanctionarea pentru derogarea de la politica stabilita conform legislatiei Romaniei sau clauzelor conventiei dintre parti.

Controlul privind indeplinirea Politicii si reanalizarea conditiilor revin Departamentului tehnologiei informationale a «PETROTEL-LUKOIL»si a companiilor din grupul Lukoil.

La finalizarea controlului «PETROTEL-LUKOIL», va intocmi un Raport conform celor constatate si-l va prezenta pentru luarea la cunostinta si avizarea acestuia S.C.I.P.

DAB 0182-28.04.11

Anexa 2
la Decizia nr.___din _____

CERINȚE
privind asigurarea securității informaționale în timpul exploatării tehnicii de calculator

1. Destinația și domeniul de aplicare

1.1.Cerințele privind asigurarea securității informaționale în timpul exploatarii tehnicii de calculator la "PETROTEL-LUKOIL" (în continuare - Cerințe) sunt destinate pentru angajații "PETROTEL-LUKOIL" (denumită în continuare "Întreprindere"), care utilizează tehnica de calculator (desktop sau laptop-uri și dispozitivele conectate la ele).
1.2. Cerințele au fost elaborate în scopul asigurării funcționării în siguranță de către angajații "PETROTEL-LUKOIL" a tehnicii de calculator și prevenirea cauzării prejudiciului intereselor Întreprinderii ca urmare a nerespectării lor.
1.3 Exploatarea de către angajații "PETROTEL-LUKOIL" a tehnicii de calculator, utilizarea de software și activitatea cu resursele informaționale trebuie să fie efectuată în așa mod, încât să excludă riscul de a provoca daune Întreprinderii și apariția altor efecte adverse.
1.4. Întreprinderea monitorizează respectarea de către angajați a acestor cerințe în timpul utilizării de către aceștia a tehnicii de calculator, software-ului instalat pe aceasta și a resurselor informaționale.

2. Cerințe privind asigurarea securității la utilizarea tehnicii de calcul

2.1. Montarea tehnicii de calculator la locul de muncă al angajatului, și, dacă este necesar, modernizarea ulterioară (înlocuirea blocurilor, achiziționarea de noi dispozitive de conectare), instalarea de software, efectuarea de modificări în software și configurarea sistemului la computerul angajatului, precum și suportul tehnic și mentenanța tehnicii de calculator, software-lui instalat pe acesta, și accesul la resursele informaționale se efectueaza in conformitate cu Contractul între "PETROTEL-LUKOIL" și "Lukoil Technology Services Romania" S.R.L. (în continuare – "L.T.S.R.") de către angajații "L.T.S.R."
2.2. Realizarea unei conexiuni nepermise a computerului la rețeua locală de calculatoare, comutarea legăturilor între prizele rețelei locale, precum și modificarea configurației hardware sau conectarea la calculator a unor dispozitive suplimentare este interzisă.

2.3. Realizarea unei conexiuni nepermise de către angajat a calculatorului la rețelele de telecomunicații care nu aparțin Întreprinderii sau firmei "L.T.S.R.", inclusiv prin intermediul unei rețele fără fir sau conexiune dial-up prin intermediul rețelelor de telecomunicații celulare, wireless si fixe (cu excepția echipamentului de calculator portabil predestinat pentru acces securizat de la distanță la resursele informaționale "PETROTEL-LUKOIL"), este interzisă.

2.4. Este interzisă realizarea conexiunii între tehnica de calcul aparţinând Întreprinderii şi dispozitive de uz personal (telefoane mobile, PDA, ş.a. – conexiune Bluetooth, infraroşu, etc.) în vederea transferului de date de orice natură.
2.5. Modificarea independentă de catre angajat a programelor şi a setărilor sistemelor software instalate pe computer, precum şi instalarea de software neautorizat este interzisă.
2.6. Se interzice folosirea suporturilor de stocare a informaţiei altele decât cele prevăzute în configuraţia sistemului angajatului (harddisk intern sau extern, CD/DVD writer intern sau extern, stick USB, etc).
2.7. În cazul în care este necesară predarea calculatorului angajatului Întreprinderii la "L.T.S.R." pentru reparaţii, trebuie să se realizeze un transfer temporar de informaţii de la aceasta la alte mijloace de informare, resurse de reţea sau la un folder la dispoziţia angajaţilor. În acest caz, toate informaţiile confidenţiale de pe calculatorul, care este predat la reparaţie trebuie să fie eliminate utilizând software-ul special de catre angajatii "L.T.S.R.", în prezenţa unui angajat al Întreprinderii.
2.7. În cazul pierderii calculatorului sau altui suport de informatii, deţinute de catre "PETROTEL-LUKOIL", angajatul Întreprinderii este obligat sa notifice imediat despre aceasta şeful ierarhic direct şi Serviciul Control Intern şi Protecţie.
2.8. Este interzisă introducerea pe teritoriul Întreprinderii a tehnicii de calcul cu caracter personal (laptopuri, etc.) fără aprobarea Serviciului Control Intern şi Protecţie.

3. Cerinţe privind asigurarea securităţii la utilizarea parolelor

3.1. Parolele personale "PETROTEL-LUKOIL" utilizate de angajaţi pentru autorizare la accesul la sistemele informaţionale, trebuie să conţină cel puţin opt caractere şi trebuie să includă o combinaţie de litere mari, litere mici, numere şi caractere speciale (@, #, $,%, ^, &, *, etc).
Un exemplu de o parolă personală: A5b # 2 & qR.
3.2. Angajaţii Întreprinderii, care utilizează parole trebuie să respecte următoarele cerinţe:
3.2.1. Se interzice să comunicaţi parolele conturilor dumneavoastră altor persoane, precum şi să le înregistraţi pe suport material, disponibile pentru alte persoane (în caz de necesitate de acces la un computer personal al unui angajat sau în caz de absenţa a lui, angajatului i se permite să dezvăluie parolele conturilor sale şefului său direct (totodată, la sosirea lui la locul de muncă, angajatul trebuie să modifice imediat aceste parole);
3.2.2. Se interzice introducerea parolei, în prezenţa altor persoane care pot observa parola introdusă;
3.2.3. Se interzice păstrarea parolei în memoria calculatorului;
3.2.4. Se interzice să se ia măsuri pentru a obţine şi utiliza parolele altor persoane (cu excepţia obţinerii şi utilizarii parolei de către şeful nemijlocit al angajatului, în conformitate cu punctul 3.2.1);
3.2.5. Înlocuirea parolelor trebuie să se efectueze nu mai puţin de o dată la trei luni (în cazul în care pe ecranul computerului apare o atare comunicare, în conformitate cu conţinutul acestui anunţ), şi în caz de suspiciune privind posibila cunoaştere a parolei de către alte persoane;
3.2.6. Parolele temporare, create de către angajatii "L.T.S.R." în timpul creării conturilor de acces sau în cazul anulării parolelor pierdute, este necesar să fie imediat modificate, iar angajatul "L.T.S.R." trebuie să informeze despre acest fapt angajatul Întreprinderii.

3.3. Anularea parolei pierdute se efectuează de către angajaţii "L.T.S.R." la solicitarea personală a angajatului a cărei parola a fost pierdută, către "L.T.S.R.", în ordinea stabilita prin Dispozitia nr АБ-54y 27.12.2000 "Cu privire la aprobarea instrucţiunii privind exploatarea mijloacelor de protecţie scriptice in componenţa locurilor de muncă automatizate a angajaţilor "PETROTEL-LUKOIL".

4. Cerinţe privind asigurarea securitatii la utilizarea postei electronice corporative

4.1. Adresa corporativă de e-mail a "PETROTEL-LUKOIL" este acordată angajatului Întreprinderii personal şi el utilizează personal acestă adresă, care i-a fost acordata, iar folosirea poştei electronice corporative nu trebuie să fie făcută în detrimentul intereselor şi imaginii Companiei şi Întreprinderii.

4.2. Utilizarea de către angajat, pe calculatorul personal a adresei de e-mail, care nu se termină în «@petrotel.lukoil.com», este permisă numai cu acordul Serviciul Control Intern şi Protecţie.

4.3. Reexpedierea informaţiilor confidenţiale de către angajat prin intermediul e-mailului se permite în modul prevăzut de Regulamentul privind protecţia informaţiilor confidenţiale în următoarele cazuri:

- Mesajul este trimis de la o adresă de e-mail corporativă, toţi destinatarii mesajului sunt localizaţi în clădirile administrative ale "PETROTEL-LUKOIL", utilizând adrese de e-mail corporative şi nu au conexiune la Internet (cu excepţia atunci când se utilizează un sistem de acces protejat la reţeaua Internet);
- Mesajul este trimis de la o adresă de e-mail corporativ, toţi destinatarii mesajului sunt situate in clădiri de oficiu, care au canale protejate de transmitere a postei electronice* cu clădirile administrative ale Întreprinderii şi utilizează adrese de e-mail corporativ;
- Mesajul este criptat de către angajat cu ajutorul mijloacelor de protecţie a corespondenţei electronice, autorizate pentru utilizare în Întreprindere. Totodată, prezenţa mijloacelor pentru decriptarea corespondenţei se precizează preliminar la destinatarii informaţiilor.

4.4. În cazurile, care nu sunt mentionate la punctul 4.3 din Cerinţe, trimiterea informaţiilor confidenţiale prin e-mail, se permite în forma de arhivă electronică cu folosirea obligatorie a unei parole (care este obligatoriu diferită de parolele de acces la conturile angajatului), care conţine cel puţin zece caractere şi include întotdeauna o combinaţie de litere mari, litere mici, numere şi caractere speciale .

4.5. Expeditorul mesajului e-mail este responsabil pentru indicarea corectă a adresei destinatarului.

5. Cerinţe privind asigurarea securităţii la utilizarea reţelei corporative de calculatoare

La utilizarea de către angajat a reţelei de calculatoare corporative a Întreprinderii este interzisă:

- Încercarea de a obţine acces la resurse şi servicii de reţele informatice corporatiste, la care angajatul nu ii este permis accesul;
- Utilizarea software specializat, destinat pentru a colecta informaţii despre reţele de calculatoare corporate (scanner de retea), ascultarea traficul de reţea (sniffer), precum şi administrarea de la distanţă (gestionarea reţelei de calculatoare corporativă);
- Crearea fără autorizaţie a resurselor de reţea (mape generale, servere Web), precum şi organizarea serviciile de reţea care introduc modificări în modul de operare al reţelei de

calculatoare corporate (servere proxy, serviciul de acces la distanță, comunicații fără fir, etc);
- Utilizarea resurselor de rețea ale Întreprinderii pentru crearea, transmiterea sau stocarea de materiale care ar putea dăuna software-ului, precum şi resursele de rețea şi alte resurse ale societății;
- Transmiterea informațiilor, care nu sunt legate de activitatea Întreprinderii.

6. Cerințe privind asigurarea securității la utilizarea rețelei Internet

La utilizarea rețelei Internet, angajatul va lua în considerație faptul, că transmiterea, precum şi căutarea şi primirea de informații, trebuie să se efectueze prin utilizarea resurselor informaționale verificate pentru a evita riscul unor consecințe negative pentru Companie, cum ar fi:
- blocarea parțială sau integrală a canalelor de transmitere a informațiilor;
- infectarea calculatoarele cu software virus, spyware, malware, troieni, etc;
- scurgeri de informații confidențiale;
- posibile încălcări ale legislatiei aplicabile, a drepturilor de autor şi conexe şi obligațiilor Întreprinderii către terți;
- posibile încălcări ale eticii şi culturii corporative;
- deteriorarea imaginii şi reputației Întreprinderii prin publicarea de informații cu privire la utilizarea de către angajații Întreprinderii a resurselor-Internet cu caracter nepotrivit.

Responsabilitatea pentru posibilele consecințe aparține angajaților "PETROTEL-LUKOIL", care accesează şi utilizează Internetul.

7. Cerințe privind asigurarea securității la utilizarea accesului de la distanță la resursele informaționale

Accesul de la distanță la resursele informaționale ale Intreprinderii poate fi acordat angajatului numai în cazul în care echipamentele utilizate pentru aceste scopuri sunt dotate cu dispozitive complexe hardware şi software de protejare a informațiilor, autorizate pentru utilizare în "PETROTEL-LUKOIL".

8. Clarificarea modului de executare a cerințelor

Pentru întrebările cu privire la executarea Cerințelor, angajații Întreprinderii se adresează pentru clarificare la Serviciul Control Intern şi Protecție.

* - Informatiile cu privire la prezenta canalelor protejate de transmitere e-mail sunt postate pe Portalul inercorporativ pe adresa : http://portalplk/dep_protectie/Documente%20Directia%20Personal/Forms/AllItems.aspx (in subcapitolul Lamuriri si raspunsuri la cele mai populare intrebari la Rubrica Securitate calculator), precum le puteti obtine si la Serviciul protectiei corporative.

DAB 0182-28.04.11

INFORMATION SECURITY POLICY[1] "PETROTEL-LUKOIL"

1.1.PASSWORD USE

Purpose and field of application

"The information security policy "PETROTEL-LUKOIL" Password use" (hereinafter called "the policy") sets out basic rules regarding the use of passwords for the access to informational assets "PETROTEL-LUKOIL" (hereinafter called "the company") or of informational assets within the company's service.

The policy will be applied in mandatorily fashion by all employees of the company and thirds using the informational assets of that.

The requirements of the hereby policy will be respected within the technical possibilities of the asset.

Policy provisions

The access to informational assets of the company or customers is carried out by the use of personal evidence recordings and passwords from numbers and letters which will be modified regularly, considering the following requirements:

- the password contains no less than eight symbols, including letters from both registers and numbers;
- the password does not have to be a word that is found in dictionaries or specialized term, including writing using another key arrangement;
- the password should not contain easily accessible information related to family, work (name, first name, date of birth, animal name, car or telephone numbers, name of organizations, email addresses, etc.);
- the password should not contain a sequence of easily discoverable numbers (123456, aaabbb, qwerty, q1w2e3, etc.).

One of the creation methods for a safe and easily memorable passwords is verse or expression coding. For example, the password created on the basis of the phrase (in Russian): "here is an example of a safe and easily memorable password" which is (could be): "Vot1PN&ZP" (in Romanian – Iata1EP&UM).

The temporary password created by the administrator in case of evidence registers or modifying the forgotten password, needs to be unique and transmitted excluding the possibility of other persons access and will be modified by the user in case of first access of the asset.

The manufacturer preset passwords will be modified before asset commissioning.

Key evidence record passwords afferent to the critical informational assets will be kept in an envelope in the safe of department leader – holder of the respective asset.

The passwords will be classified as trade secrecy and will be kept according to classified information protection regulations.

THE FOLLOWING ARE FORBIDDEN:

- communicating to other persons the personal password or its writing on a material support accessible to other persons (except when it is foreseen to keep the passwords of the key registrations by the asset holder);
- keeping passwords when the technical means are in operation or using the automatic means of entry;

[1] By the information security in the hereby document, organisational and technical actions are understood with regard to information security from thirds unauthorised access

- using an easy-to-find password modification algorithm (for example, F%1hTR8 → F%2hTR8 → F%3hTR8, or F%1hTR8 → F1%hTR8 → F1h%TR8, etc.);
- using other people's evidence records;
- using passwords outside the company that coincide with passwords for access to its informational assets;
- using the examples in this document as a password.

The password will be changed every 6 months or in case of finding compromise situations, and regarding the administrative evidence records – together with the change of the person who performs the functions of administrator.
The passwords will be prepared by «PETROTEL-LUKOIL» and will be endorsed by S.C.I.P.
According to the critical character of the technical-informational asset, the holder can set higher demands on the complexity of the password and the frequency of its modification. The processes of creating, modifying, using, blocking, cancelling the records, as well as modifying the passwords will be regulated, provided that the control over these processes is exercised and reports prepared.

Roles and obligations

The obligation regarding the observance of the provisions of this policy is the responsibility of all the employees of the company and thirds who use the technical-informational assets, the informational assets that are in the company service. All derogations from the policy will be approved by the information technology department, S.C.I.P. and also with the departments responsible for protecting the information of the customers transferring the informational assets in the company service from the unauthorized access, and the unapproved derogations will be considered incidental and can serve as the basis for the sanction for the derogation from the policy established according to the Romanian legislation or the clauses of the convention between the parties.
The control regarding the fulfilment of the policy and the re-analysis of the conditions, are the responsibility of the information technology department of «PETROTEL-LUKOIL» and of the companies in the Lukoil group.
After conducting the inspection, «PETROTEL-LUKOIL» will prepare a report on the violations found, the report will be presented to S.C.I.P. for its recognition and endorsement and it will be presented later to the company management.

1.2.ACCESS MANAGEMENT

Purpose and field of application

"The information security policy" PETROTEL-LUKOIL "Access management" (hereinafter called "the policy") establishes the basic rules and requirements regarding the organization and access control of company employees and thirds (hereinafter called "users") to the information technology assets that support the business processes of "PETROTEL-LUKOIL".
The information technology assets include information resources, business applications, services (for example, e-mail, Internet, telephony) and other technological components of the Company's informational infrastructure.
The policy is valid for the employees of the company who have the status of holders of the information technologic assets or who manage the access to them and it is mandatory for fulfilment.

Policy provisions

Each information technology asset must be assigned to an employee from the department within the structure, whose obligation is to establish and revise the rules of compliance for access management and control. The access to the information technology asset is granted following the decision of its holder according to the procedure established by the owner and approved by

the Information Security Department and S.C.I.P. regarding access granting, as well as by the person who manages the access rights of users to the information technology asset (hereinafter called "administrator"). Access to the information technology assets must be granted after the assessment of the related risks according to the business requirements and the functional obligations of the users, if it is possible according to the group, those that include users with adjacent functional obligations.
The use of access to information technology assets must be controlled and reports must be drafted on the subject matter with users aware of their responsibility in the case of using them illegally and they must comply with the requirements regarding their protection established by the holders of information technology assets.
The access rights of the users must be regularly analysed by the holders of the information technology assets in order to highlight the exceeded or surplus rights, and the access of the dismissed or transferred company employees and thirds who have concluded their activity based on agreements which must be revised or terminated. Automated access management systems must contain management mechanisms by recording data and must operate based on the standard user authorization procedure that uses recorded data and password.
Access to information technology assets with the use of registration data without a password is prohibited, and the use of registration data with administration rights and access to utilities by means of diagnostic system must be subject to special control by the holder of the information technology asset. Software that supports critical business processes must be logically grouped and separated from others (for example, with the use of inbound screens), and the connection of software that processes strictly confidential information to telecommunications networks, is prohibited.
Mechanisms must be used when using remote or wireless access intensified authentication, coding and verification of the automated station configuration from a distance regarding compliance with security requirements.
Component, architecture and configuration of software means used for access management must be standardized, and the processes of their installation, setting, activation, commissioning and updating must be regulated, provided in protocols and controlled.

Who is responsible?
Company employees that perform the functions of the holders of information technology assets or performing access management to them, are responsible for compliance with the provisions of the policy.
All derogations from the policy must be agreed with the Information Security Department. The unauthorized deviations from the provisions of this policy are considered incidents in the field of information security and may be the basis for taking responsibility according to the Romanian legislation or the agreement between the parties.
The policy fulfilment control and its updating are the responsibility of S.C.I.P of «PETROTEL-LUKOIL» and of the companies in the Lukoil group. The results of the control will be presented by «PETROTEL-LUKOIL» on the basis of S.C.I.P. reports, for its recognition and approval.
The supervision of these policies fulfilment and the controls is performed by «PETROTEL-LUKOIL» with the responsibility of the Internal Control and Protection Service.

1.3.USE OF ELECTRONIC MAIL

Designation and field of application
"Information security policy" PETROTEL-LUKOIL "regarding the use of electronic mail" (hereinafter called "the policy") sets the core rules and requirements for the protection of

information assets and the reputation of "PETROTEL-LUKOIL" (hereinafter called "the company") against threats related to the use of electronic mail.
The policy is valid for all employees of the company and thirds who use the software and hardware means of the company to receive or transmit messages by electronic mail and whose implementation is mandatory.

Policy provisions
The use of the electronic mail must be authorized according to the procedure in force regarding the access granting to informational assets and that is carried out by electronic mail addresses of the Company.
The use of electronic mail should only be performed in order to carry out the functional tasks. Confidential information transmitted through the use of electronic mail must be protected from unauthorized viewing or modification. The transmission of strictly confidential information is prohibited by electronic mail.
It is forbidden to use the electronic mail in a manner disrespecting the regulations in force, corporate ethics and culture, as well as the copyrights and related rights of other persons or which represent any form of identity tracking. Actions for sending and receiving e-mail messages must be recorded and the messages must be saved.
In the e-mail messages sent to thirds recipients, the information that exonerates the company responsible for the content of the message must be added and that it prevents the recipient of the message from responding for the unlawful use of the message.
Steps must be taken to prevent the transmission of unrequested anonymous messages, including those with advertising character (spam). Before sending e-mail messages, the correctness of the recipients' addresses must be verified.
The company reserves the right not to transmit the message if the requirements of the policy are not met. The content, architecture and configuration of the company's e-mail servers must be standardized and their installation, setup, activation and operation with updating processes regulated, controlled and registered.

Roles and responsibilities
Responsibility for compliance with the policy lies with all employees of the company and thirds using the software and hardware means of the company for sending and receiving emails. All exceptions to the policy must be agreed with the Department of Information Technology. The unauthorized deviations from the provisions of the policy are considered incidents of informational security and may have the core of being held liable according to the Romanian legislation or the agreement between the parties.
The control regarding the fulfilment of the policy and its revision is the responsibility of the Information Technology Department of «PETROTEL-LUKOIL» and of the companies in the Lukoil group. The control results will be notified to S.C.I.P. by «PETROTEL-LUKOIL», in the form of a report which will be later approved.

1.4.USE OF INTERNET

Designation and field of application
"Information security policy" PETROTEL-LUKOIL "regarding the use of internet" (hereinafter called "the policy") sets the core rules and requirements for the protection of information assets and the reputation of "PETROTEL-LUKOIL" (hereinafter called "the company") against threats related to the use of internet.
The policy is valid for all employees of the company and thirds who use the software and hardware means of the company to access the internet and whose implementation is mandatory.

Policy provisions

Access to the Internet must be authorized according to the procedure in force regarding access granting to information assets.

The access to the Internet should be done only for the fulfilment of the functional tasks. Confidential information transmitted through the use of the Internet must be protected from unauthorized viewing or modification. The transmission of strictly confidential information by using the Internet is prohibited.

It is forbidden to use the Internet in a manner that breaches the regulations in force corporate ethics and culture, as well as the copyrights and related rights of other persons.

The use of the Internet is prohibited for the purpose of publishing information on behalf of the company without the approval of the management. The content and volume of information transmitted or retrieved through the use of the Internet may be limited.

The company reserves the right to monitor the use of the Internet in order to comply with the provisions of the policy.

The content, architecture and configuration of the software and hardware means used to retrieve or transmit information through the Internet must be standardized and the processes of installation, setup, activation, operation and updating must be regulated, controlled and recorded.

Roles and responsibilities

Responsibility for compliance with the policy lies with all employees of the company and thirds using the software and hardware means of the company for internet. All exceptions to the policy must be agreed with the Department of Information Technology. The unauthorized deviations from the provisions of the policy are considered incidents of informational security and may have the core of being held liable according to the Romanian legislation or the agreement between the parties.

The control regarding the fulfilment of the policy and its revision is the responsibility of the Information Technology Department of «PETROTEL-LUKOIL» and of the companies in the Lukoil group. The control results will be notified to S.C.I.P. by «PETROTEL-LUKOIL», in the form of a report which will be later approved.

1.5.INVENTORY OF INFORMATION ASSETS

Purpose and field of application

"Information security policy" PETROTEL-LUKOIL "regarding the information assets inventory" (hereinafter called "the policy") sets the core rules and requirements for identification and designation of persons responsible with core information assets of "PETROTEL-LUKOIL" (hereinafter called "the company").

The policy will be applied in mandatorily fashion by department leaders from the company structure, employees within the services assuring information security and employees designated by holders of information assets.

Policy provisions

Inventory of the informational assets will be carried out within the company's departments before commissioning, as well as annually, according to the unitary method approved by the company management.

All key informational assets of the company will be identified with the damages caused due to the breach of the security rules and with the person from the department that will perform the functions of the owner, will be designated.

Obligations of the holder of the informational asset:

- presenting the necessary data regarding the asset for the purpose of registration in the register with informational assets, risk assessment, planning the continuity of the activity under conditions of dysfunctions and disasters;
- classifying information, establishing and re-analysing access management rules, as well as granting and terminating the right of access to the information asset;
- the application regarding the information assets of the security measures provided in the policies, regulations and instructions of the company regarding the provision of information security, as well as in the Risk Management Plan;
- establishing and controlling the application of the security requirements of the information assets by the users within the company and thirds as well.

In case the delegation of a part of the obligations by the owner (for example, the administration of the users' competences, the management of the technical means of security) to a specialized department, this will be recorded in the Register of informational assets, and the task regarding ensuring the security of the informational asset remains the obligation of the respective holder.

Roles and obligations

The obligation regarding the inventory and completion of the information assets register is the responsibility of the information security departments.

The obligation regarding the designation of the holders of the informational assets and their replacement in the case of the personnel changes is the responsibility of the managers of the departments in the structure.

The obligation regarding the security of the information assets is the responsibility of the holders. The unauthorized deviations from the provisions of the policy are considered incidents of informational security and may have the core of being held liable according to the Romanian legislation or the agreement between the parties.

The control regarding the fulfilment of the policy and its revision is the responsibility of the Information Technology Department of «PETROTEL-LUKOIL» and of the companies in the Lukoil group. The control results will be notified to S.C.I.P. by «PETROTEL-LUKOIL», in the form of a report which will be later approved.

Annex No. 17
To Specification Batch No. 1-4

Appendix 2
To the decision no. _____ of _____

REQUIREMENTS
regarding the information security assurance during IT equipment commissioning

1. Designation and field of application

1.1. Requirements regarding the assurance of information security during the commissioning of IT equipment at "PETROTEL-LUKOIL" (hereinafter called requirements) are intended for "PETROTEL-LUKOIL" employees (hereinafter called "the company"), who uses IT equipment (desktops or laptops and devices connected to them).

1.2. The requirements have been developed in order to ensure the safe operation by "PETROTEL-LUKOIL" employees at IT equipment and the prevention of company damage interests as a result of non-compliance.

1.3. The commissioning by the "PETROTEL-LUKOIL" employees of IT equipment, the use of software and the activity with the information resources must be carried out in such a way as to exclude the risk of causing damage to the company and prevent the occurrence of other adverse effects.

1.4. The company monitors the compliance of employees with these requirements during the use of IT equipment, the software installed on it and information resources.

2. Requirements regarding security assurance upon IT equipment use

2.1. Installing IT equipment at the employee's workplace, and, if necessary, further upgrading (replacing blocks, purchasing new connection devices), installing software, making software changes and configuring the system on the employee's computer, as well as technical support and maintenance of the IT equipment, with the software installed on it, and access to information resources, are made in accordance with the agreement between "PETROTEL-LUKOIL" and "Lukoil Technology Services Romania" SRL (hereinafter called "L.T.S.R.") by the employees of "L.T.S.R.".

2.2. Making an unauthorized connection of the computer to the local computer network, switching the connections between the local network outlets, as well as changing the hardware configuration or connecting additional devices to the computer is prohibited.

2.3. Making an unauthorized connection by the employee from the computer to the telecommunications networks that do not belong to the company or the "LTSR" company, including through a wireless network or dial-up connection through the cellular, wireless and fixed telecommunications networks (except for the portable computer predestined for remote access to information resources "PETROTEL-LUKOIL"), is forbidden.

2.4. It is forbidden to make the connection between the computing technique belonging to the company and for personal use devices (mobile phones, PDA, etc. - Bluetooth, infrared connection, etc.) in order to transfer data of any kind.

2.5. Employee independent modification of software and software system settings installed on the computer as well as unauthorized software installation is prohibited.

2.6. It is forbidden to use information storage media other than those provided in the employee's system configuration (internal or external hard disk, internal or external CD/DVD writer, USB stick, etc.). If it is necessary to hand over the company employee's computer to the "L.T.S.R." for repairs, a temporary transfer of information from it to other means of information, network resources or a folder available to employees must be made. In this case, all confidential information on the computer, which is handed

over to the repair, must be removed using the special software by the employees "L.T.S.R.", in the presence of an employee of the company.

2.7. In case of loss of the computer or other information medium, held by "PETROTEL-LUKOIL", the employee of the company is obliged to immediately notify the direct manager and the Internal Control and Protection Service about this.

2.8. It is forbidden to introduce in the territory of the company the calculation technique with personal character (laptops, etc.) without the approval of the Internal Control and Protection Service.

3. Requirements regarding security assurance on password use

3.1. Personal passwords "PETROTEL-LUKOIL" used by employees for authorization to access information systems, must contain at least eight characters and must include a combination of capital letters, lowercase letters, numbers and special characters (@, #, $,% , ^, &, *, etc). An example of a personal password: A5b # 2 & qR.

3.2. Employees of the company, who use passwords must comply with the following requirements:

3.2.1. It is forbidden to communicate passwords of your accounts to other persons, and to register them on material support, available to other persons (in case of access need to an employee's personal computer or in case of his absence, the employee is allowed to disclose the passwords of his/her accounts to his/her direct boss (at the same time, upon arrival at the workplace, the employee must immediately change these passwords);

3.2.2. It is forbidden to enter the password, in the presence of other people who can observe the entered password;

3.2.3. It is forbidden to keep the password in the computer memory;

3.2.4. It is forbidden to take measures to obtain and use the passwords of other persons (except for obtaining and using the password by the direct boss of the employee, in accordance with point 3.2.1);

3.2.5. Passwords should be replaced no less than once every three months (if such communication appears on the computer screen, according to the content of this notice), and in case of suspicion regarding the possible knowledge of the password by other persons;

3.2.6. The temporary passwords, created by the "L.T.S.R." employees during the creation of the access accounts or in the case of cancellation of lost passwords, need to be changed immediately, and the "L.T.S.R." employee must notify the employee of the company about this.

3.3. The cancellation of the lost password is performed by the "LTSR" employees at the personal request of the employee whose password was lost, to "LTSR", in the order established by the Provision no. АБ-54у 27.12.2000 scripted protection in the composition of the automated work places of "PETROTEL-LUKOIL" employees.

4. Requirements regarding security assurance at corporate email use

4.1. The corporate e-mail address of "PETROTEL-LUKOIL" is given to the employee of the company personally and he personally uses this address, which was granted to him, and the use of the corporate electronic mail should not be made to the detriment of the interests and image of the company.

4.2. The use by the employee, on the personal computer of the email address, which does not end in «@ petrotel.lukoil.com», is allowed only with the agreement of the Internal Control and Protection Service.

4.3. The re-sending of confidential information by the employee by e-mail is permitted in the manner provided by the regulation on the protection of confidential information in the following cases:

- The message is sent from a corporate email address, all the recipients of the message are located in the administrative buildings of "PETROTEL-LUKOIL", using corporate email addresses and have no Internet connection (except when using a system protected access to the Internet);
- The message is sent from a corporate e-mail address, all the recipients of the message are located in office buildings, which have protected channels of electronic mail transmission * with the administrative buildings of the company and use corporate e-mail addresses;
- The message is encrypted by the employee using the means of protection of electronic mail, authorized for use in the company. At the same time, the presence of the means for decrypting the correspondence is specified preliminary to the recipients of the information.

4.4. In the cases, which are not mentioned in point 4.3 of the requirements, the sending of confidential information by e-mail is allowed in the form of an electronic archive with the obligatory use of a password (which is mandatory different from the passwords of access to the employee's accounts), which contains at least ten characters and always includes a combination of capital letters, lowercase letters, numbers and special characters.

4.5. The sender of the e-mail is responsible for correctly indicating the address of the recipient.

5. Requirements regarding security assurance at corporate network use

At the employee's use of the corporate computer network of the company the following is prohibited:

- Attempting to gain access to corporate IT resources and services, to which the employee is not allowed access;
- The use of specialized software, designed to collect information on corporate computer networks (network scanner), listening to network traffic (sniffer), as well as remote administration (management of corporate computer network);
- Creation without authorization of the network resources (general maps, web servers), as well as the organization of the network services that introduce changes in the operating mode of the network of corporate computers (proxy servers, remote access service, wireless communications, etc.);
- Use of the enterprise's network resources for creating, transmitting or storing materials that could harm the software, as well as the network resources and other resources of the company;
- Transmission of information that is not related to the activity of the company.

6. Requirements regarding security assurance at Internet use

When using the Internet network, the employee will take into account the fact that the transmission, as well as the search and reception of information, must be done by using the verified information resources to avoid the risk of negative consequences for the company, such as:

- partial or complete blocking of information transmission channels;
- infecting computers with virus, spyware, malware, Trojans, etc;
- leakage of confidential information;

- possible violations of the applicable legislation, copyright and related rights and obligations of the company to thirds;
- possible violations of corporate ethics and culture;
- deterioration of the image and reputation of the company by publishing information regarding the use by the employees of the Company of the Internet resources of inappropriate character.

The responsibility for the possible consequences lies with the "PETROTELLUKOIL" employees, who access and use the Internet.

7. Requirements regarding security assurance at remote access to information resources use

Remote access to the company's information resources may be granted to the employee only if the equipment used for these purposes is endowed with complex hardware and software for protecting information, authorized for use in "PETROTEL-LUKOIL".

8. Clarification of requirements performance method

For questions regarding the performance of requirements, company employees should address the Internal Control and Protection Service for clarification.

* - The information regarding the presence of the protected channels of e-mail transmission are posted on the Inertial Portal at: http://portalplk/dep_protectie/Documents%20Directia%20Personal/Forms/AllItems.aspx (in the subsections and answers to the most popular questions. at Computer Security), and you can also get them from the Corporate Protection Service.