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 I. Kuzmin

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

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 şi 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 şi 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 şi 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 şi activitatea cu resursele informaționale trebuie să fie efectuată în aşa mod, încât să excludă riscul de a provoca daune Întreprinderii şi apariția altor efecte adverse.
1.4. Întreprinderea monitorizează respectarea de către angajați a acestor cerințe în timpul utilizării de către aceştia a tehnicii de calculator, software-ului instalat pe aceasta şi 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, şi, dacă este necesar, modernizarea ulterioară (înlocuirea blocurilor, achiziționarea de noi dispozitive de conectare), instalarea de software, efectuarea de modificări în software şi configurarea sistemului la computerul angajatului, precum şi suportul tehnic şi mentenanța tehnicii de calculator, software-lui instalat pe acesta, şi accesul la resursele informaționale se efectueaza in conformitate cu Contractul între "PETROTEL-LUKOIL" şi "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 şi 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.