LUKOIL OIL COMPANY

PETROTEL-LUKOIL S.A.

DAB 0098-03.04.19

D E C I Z I E

Privind aprobarea Regulamentului privind asigurarea securitatii informationale in PETROTEL-LUKOIL S.A. si respectarii acestuia de catre personalul PLK si societatile terte

DAB 0098-03.04.19

In scopul executarii Deciziei CP LUKOIL nr.226 din 11.12.2018 pentru aprobarea Regulamentului privind asigurarea securitatii informationale in expluatarea tehnicii de calcul de catre angajatii Grupului LUKOIL,

DECID:

1. Se aproba Regulamentul privind asigurarea securitatii informationale in PETROTEL-LUKOIL S.A. (Anexa 1).
2. Sefii compartimentelor structurale pana la data de 15.04.2019 vor aduce la cunostinta subordonatilor Regulamentul privind asigurarea securitatii informationale (Regulament), prin proces verbal cu semnaturile angajatilor, care va fi transmis catre Serviciul Protectie Corporativa (Anexa 2).
3. Departamentul personal si probleme generale:
   - va aduce la cunostinta studentilor/elevilor pana la inceperea practicii pe teritoriul rafinariei, prevederile Regulamentului, prin Proces verbal cu semnaturile acestora, care va fi transmis catre Serviciul Protectie Corporativa.
   - va aduce la cunostinta persoanelor noi angajate prevederile Regulamentului prin Proces verbal cu semnaturile acestora, care va fi transmis catre Serviciul Protectie Corporativa.
4. Responsabilii de incheierea contractelor cu firmele terte vor aduce la cunostinta acestora prevederile Regulamentului, in dependenta de activitatea desfasurata conform obiectul contractului. La necesitate vor include punctele aferente din Regulament in Obligatiile contractorului.
5. Decizia va fi adusa la cunostinta tuturor angajatilor societatii.

6. Se anuleaza Decizia nr. DAB-0211 din 04.05.2012 privind aprobabrea Regulamentului de asigurarea a securitatii informationale.

7. Controlul executarii prezentei decizii imi apartine.

Presedinte al Directoratului - Director General Executiv

A. Kovalenko

DAB 0098-03.04.19

I.Spataru
34363

LISTA DE AVIZARE

În Decizie: PRIVIND APROBAREA REGULAMENTULUI PRIVIND ASIGURAREA SECURITATII INFORMATIONALE IN PETROTEL-LUKOIL S.A. SI RESPECTARII ACESTUIA DE CATRE PERSONALUL PLK SI SOCIETATILE TERTE

INITIAT DE:

Sef Serviciu Protectie Corporativa	I.Besciotnii	03/04/2019 12:33:07	Finalizare

AVIZAT DE:

APROBAT
Prin Decizia Nr.____
din __.__20 .

REGULAMENT CU PRIVIRE LA ASIGURAREA SECURITATII INFORMATIONALE IN PETROTEL-LUKOIL S.A.

CODUL DOCUEMNTULUI: ____

Editia: 2 / __.__2019

	Nume si prenume	Functia	Semnatura	Data
AVIZAT	BESCIOTNII IGOR	Sef Serviciu Protectie Corporativa		
VERIFICAT	ANDREI CRISTINA	Specialist Certificare		
INTOCMIT	SPATARU ION	Specialist SIG/IT		

Copie in evidenta		Ex. nr.	

PAGINA DE EVIDENTA A EDITIILOR / REVIZIILOR		
Titlul documentului: REGULAMENT CU PRIVIRE LA ASIGURAREA SECURITATII INFORMATIONALE IN PETROTEL-LUKOIL S.A. **Tipul documentului / sistemul caruia i se aplica: Regulament/ Sistemе de management**	**Cod document:** **___** **Ed.: 2/.....**	**Pag.: 2 / 18** **Rev.: 0/.....** **Ex. nr.:**

Pag. / Revizie																
Pag.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Revizia	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Pag. / Revizie																
Pag.	17	18	19													
Revizia	0	0	0													

SITUATIA REVIZIILOR PAGINILOR

Paragraf / Pag.	Ed. / Rev.	Modificarea operata	Justificarea modificarii

	Numele si Prenumele	Functia	Semnatura	Data
Aprobat				
Avizat				
Verificat				
Intocmit				

CUPRINS

1. **Scopul, obiectivele si domeniul de actiune** 3
2. **Incidentele de securitate a informațiilor** 4
3. **Echipamente informatice și echipamente de birou** 5
4. **Regulile utilizarii softului** 7
5. **Medii de stocare a informatiilor** 8
6. **Conturi** 9
7. **Retele de calculatoare corporative si resurse informationale** 9
8. **Regulile utilizarii postei electronice** 10
9. **Protecția parolei** 11
10. **Protecție împotriva codului rău intenționat (malware)** 13
11. **Internet și rețele** 13
12. **Serviciul Cloud** 14
13. **Protectia datelor cu caracter personal (GDPR)** 15
14. **Restrictii legislative si normele eticii corporative** 16
15. **Asistenta tehnica** 17
16. **Explicarea modalitatii de indeplinire a Regulamentului** 18

1. Scopul, obiectivele si domeniul de actiune

1.1. Regulamentul pentru asigurarea securității informațiilor în funcționarea echipamentelor informatice și de birou (denumite în continuare Regulament/Cerințe) sunt respectate de catre angajații societatii PETROTEL-LUKOIL (in continuare PLK) si ai firmelor terte, de catre persoanele care desfășoară activități în baza contractelor de drept civil cu organizațiile Grupului LUKOIL și de catre elevii / studentii din institutiile de invatamant, admisi pentru stagiere in cadrul societatii PLK (denumiti în continuare în mod colectiv - angajați).

1.2. Scopul Regulamentului este de a asigura confidențialitatea și integritatea informațiilor societatii PETROTEL-LUKOIL, precum și de a asigura continuitatea accesului la acestea.

1.3. Obiectivele Regulamentului sunt urmatoarele:

- îndeplinirea acțiunilor obligatorii ale angajaților in procesul de utilizare a echipamentelor informatice și de birou;
- cresterea nivelului de cunostinte a lucrătorilor în domeniul riscurilor de securitate a informațiilor;
- prevenirea producerii și / sau reducerea daunelor cauzate de incidentele de securitate a informațiilor, precum și crearea condițiilor pentru detectarea și notificarea în timp util a serviciilor interesate cu privire la incidentele de securitate a informațiilor în caz de apariție a acestora;
- formalizarea riscurilor, precum și procedurile de control, care stabilesc responsabilitatea angajaților cu privire la respectarea obligatorie a normelor stipulate în Regulament și care vizează reducerea riscurilor de mai sus.

1.4. Regulamentul nu se aplică prelucrării informațiilor clasificate drept secrete de stat, ci în ceea ce privește sistemele de informații care gestioneaza informatii cu caracter personal și obiectelor de infrastructură critică care nu contravine cerințelor stabilite de legislatie în domeniul securității precum si în domeniul combaterii spionajului tehnic.

1.5. În ceea ce privește informațiile clasificate ca fiind confidențiale de către o terță parte, aceste cerințe sunt aplicate în măsura în care nu contravin actelor normative locale ale proprietarului de drept și acordurilor bilaterale cu aceasta.

2. Incidentele de securitate a informațiilor

2.1. Un eveniment de securitate a informațiilor reprezinta o situație identificată a stării unui sistem informatic sau a unei rețele de calculatoare, care indică o eventuală încălcare a politicii de securitate a informațiilor, eșecul măsurilor de protecție și apariția unei situații necunoscute anterior care ar putea fi legată de securitate.

2.2. Incidentul în materie de securitate a informațiilor inseamna apariția unuia sau mai multor evenimente nedorite sau neașteptate legate de securitatea informațiilor, care sunt asociate cu o probabilitate semnificativă de compromitere a operațiunilor de afaceri și crearea unei amenințări de încălcare a securității informațiilor.

2.3. Exemple de incidente de securitate a informațiilor includ:

- accesul neautorizat la informații protejate, echipamente, mijloace media, direct sau prin rețea;
- pierderea sau furtul de mijloace media de informații confidențiale, chei, parole;
- accesul la informații care, în opinia angajatului, nu ar trebui să i se pună la dispoziție;
- detectarea informațiilor protejate la persoanele neautorizate pentru accesul la acestea, fie în acces liber, inclusiv în rețelele sociale, în mass-media electronice;
- abateri de la prevederile acestor cerințe care nu au fost preliminar avizate cu departamentul de securitate corporativă.

O listă detaliată a incidentelor de securitate a informațiilor este prezentată în Regulamentul cu privire la prelucrarea incidentelor de securitate informationala in PETROTEL – LUKOIL S.A..

2.4. Dacă un incident de securitate a informațiilor este detectat, angajatul trebuie:

- sa nu intreprinda măsuri independente pentru a opri incidentul, pentru a identifica vinovatul, pentru investigarea sau eliminarea vulnerabilității pe baza careia acest incident a avut loc;
- sa inregistreze pe cât posibil si în orice mod posibil circumstanțele incidentului;
- sa raporteze incidentul la Serviciul de asistență tehnică sau la responsabilul de gestionarea incidentelor de securitate a informațiilor din cadrul organizației sale, precizând că adresarea s-a realizat din cauza unui incident de securitate informationala;
- să nu divulge informații despre incident altor persoane, cu excepția angajaților compartimentului de securitate corporativă și a specialiștilor tehnici implicați în gestionarea incidentului.

2.5. Pentru a raporta un incident de securitate a informațiilor, este de preferat să se foloseasca comunicarea bidirecțională (telefonul fix sau telefonul mobil) pentru ca în acest caz, responsabilul de incidente poate ajusta cantitatea de informații primare înregistrate în aplicație, în conformitate cu instrucțiunile pe care le poseda și poate informa, de asemenea, angajatul cu privire la acțiunile ulterioare.

3. Echipamente informatice și echipamente de birou

3.1. Echipamentele computerizate și periferice, mijloacele de comunicație, echipamentele de birou sunt furnizate angajaților numai pentru îndeplinirea sarcinilor de lucru prevăzute în fisele lor de post, in contract sau in programul de stagiere și este interzisa utilizarea acestora în alte scopuri.

3.2. Utilizarea echipamentelor personale ale angajaților pentru îndeplinirea sarcinilor de lucru trebuie autorizată de Serviciul protectie corporativă și efectuată în condițiile stabilite de acest serviciu.

3.3. Este interzisă crearea, primirea, transmiterea, stocarea sau utilizarea datelor care încalcă restricțiile legale și etica corporativă privind echipamentele din PLK și echipamentele personale permise de Serviciul protecte corporativa pentru utilizarea în activitatea de munca.

3.4. Instalarea, conectarea, reglarea echipamentelor din PLK, schimbarea configurației sale hardware, precum și conectarea dispozitivelor periferice la acestea vor fi efectuate de către personalul organizațiilor care furnizează servicii de suport și asistenta pentru echipamente, la cererea angajatului adresata către Serviciul de Asistență Tehnică.

3.5. Este interzisă modificarea independentă a configurației hardware a echipamentelor din PLK, precum și activarea și dezactivarea componentelor acestora, conectarea la acestea a dispozitivelor periferice, efectuarea lucrărilor de întreținere sau modernizare fara autorizarea compartimentului de securitate corporativa.

3.6. Este interzisă modificarea independentă a configurației hardware a echipamentelor personale permise pentru utilizarea în activitățile de lucru precum și activarea și dezactivarea componentelor sale, conectarea dispozitivelor periferice la aceasta, repararea sau modernizarea acestora, fara autorizarea Serviciului protectie corporativa.

3.7. În clădiri de birouri din PLK și in cazul in care este permis de compartimentul de securitate corporativa si in afara acestor cladiri, angajații trebuie să utilizeze echipamentul în așa fel încât să împiedice vizualizarea informațiilor afișate pe ecran, introduse din tastatură sau transmise la imprimat, de catre alte persoane straine, care nu au acces primit in acest sens.

3.8. Atunci când părăsesc temporar echipamente fara a le monitoriza, accesul nesupravegheat la monitor și dispozivele de intrare-ieșire trebuie sa fie blocat (în sistemul de operare Windows - aceasta este combinația de taste «windows» și «L» sau «Ctrl», «Alt» și «Del», dupa care selectați "Blocare"), pentru dispozitive mobile sa fie activat modul de solicitare a unei parole de caractere sau a unei parole grafice când ecranul este activat.

3.9. Angajaților li se interzice accesul la echipamente care sunt folosite de alți angajați, cu excepția cazului în care accesul este permis cu avizarea de catre sefii direcți ai acestor angajați.

3.10. La finalizarea operării echipamentului (predarea în depozit, transferul autorizat către un alt angajat, transferul către reparații) angajații trebuie să elimine informațiile confidențiale și setările de acces din acesta.

3.11. Regulile pentru introducerea și scoaterea echipamentelor prin intermediul punctelor de control sunt stabilite de actele de reglementare locala (dacă există) privind regimul de control al accesului și regimului intern al organizației-proprietar al clădirii administrative corespunzătoare.

3.12. În clădirile administrative ale PETROTEL-LUKOIL, se poate admite introducerea / scoaterea unica si operarea echipamentului informatic portabil fără acces la informațiile confidențiale ale organizațiilor din PLK și fără conexiune la rețeaua corporatista, pe baza cererii trimise sau pe baza unei cereri scrise adresate șefului compartimentului responsabil, semnată de șeful unității structurale într-o poziție de cel putin sef de departament, șef al organizației chiriase sau a organizației de prestare servicii.

3.13. Introducerea/ scoaterea regulata si operarea dispozitivelor mobile (in continuare DM) in cladirile administrative ale PLK se realizeaza pe baza autorizatiilor emise de Serviciul protectie corporativa. Permisele pentru introducerea/ scoaterea regulată si exploatarea DM sunt emise de Serviciul protectie corporativa pe baza unei cereri adresate conducătorului Serviciului de securitate corporativă.

3.14. În absența unei autorizații, utilizarea DM în clădirile administrative ale organizațiilor din grupul LUKOIL este interzisă.

3.15. Înainte de a utiliza DM pentru procesarea sau stocarea informațiilor confidențiale ale organizațiilor din PLK, dispozitivul trebuie să fie configurat de un angajat al Serviciului de asistență tehnică în conformitate cu regulamentul de securitate a informațiilor.

3.16. În absența capacității tehnice de a seta un echipament informatic portabil în conformitate cu cerințele securității informaționale, acesta nu poate fi utilizat în scopul stocării și prelucrării informațiilor confidențiale ale PETROTEL-LUKOIL.

3.17. În afara clădirilor administrative, angajatul este obligat să ia toate măsurile necesare pentru a preveni furtul de echipamente și accesul la acestea de către persoane neautorizate.

3.18. Pierderea unui dispozitiv portabil de calcul sau a unui dispozitiv mobil ce apartine societatii PETROTEL-LUKOIL, precum și a unui dispozitiv personal utilizat în activitățile de producție etc., cu permisiunea unității de securitate corporativă, reprezinta un incident de securitate a informațiilor, iar angajatul este obligat să acționeze în conformitate cu punctul 2.4.

4. Regulile utilizarii softului

4.1. Instalarea, configurarea, dezactivarea sau stergerea software-ului de pe echipamentul societatii PETROTEL-LUKOIL trebuie să fie efectuata de către personalul organizațiilor care furnizează servicii de suport la solicitarea angajatului adresata catre Serviciul de asistență tehnică.

4.2. La echipamentele PLK, angajații nu au dreptul să creeze, să instaleze, să configureze, să dezactiveze sau să șteargă software-ul in mod independent, să stocheze și să utilizeze software care nu le-a fost furnizat sau configurat de Serviciul de asistență tehnică.

4.3. Angajaților li se interzice configurarea, dezactivarea sau eliminarea software-ului furnizat sau prescris pentru utilizare de către Serviciul protectie corporativă, pe echipamentele personale care sunt permise pentru utilizarea în activitățile de producție.

4.4. Pe echipamentul din PLK și echipamentului personal autorizat pentru utilizare în activitățile de producție, se interzic urmatoarele:

- crearea, primirea, transferul, instalarea, stocarea sau utilizarea de software care încalcă restricțiile legale și etica corporativă;
- utilizarea de software conceput pentru accesul neautorizat la informații, gestionarea ascunsă a unui computer la distanță, ascultarea traficului de rețea, căutarea sau exploatarea vulnerabilităților site-ului și ale dispozitivelor de rețea.

4.5. Atunci când utilizeaza dispozitive personale pentru a efectua sarcini de producție, angajatul nu trebuie să împiedice actualizarea automată a software-ului antivirus, software-ului de aplicație și de sistem, inclusiv a mijloacelor prescrise de protecție a informațiilor procesate pe dispozitiv.

4.6. Instalarea, configurarea, deconectarea și eliminarea software-ului, conectarea și deconectarea dispozitivelor externe la calculator, exercitate de către angajatii unităților de IT în scopul testării, sunt permise cu condiția ca șeful respectivului compartiment sa aprobe planul de testare și de organizare a mediului de testare, izolat fizic sau virtual, fie cu avizarea Serviciului protectie corporativă.

5. Medii de stocare a informatiilor

5.1. Pentru a îndeplini sarcinile de serviciu, angajații trebuie să folosească medii de stocare incorporate și externe, furnizate de catre PLK.

5.2. În lipsa unei alte posibilități de transfer al fișierelor referitoare la activitățile de serviciu, este permisă utilizarea o singura data a suporturi media externe si personale, în următoarele condiții:

- suporturile media externe sunt sterse de orice alte informații;
- fișierele înregistrate nu conțin informații confidențiale suportul carora face obiectul evidentei obligatorii;
- suportul nu este transmis persoanelor care nu sunt autorizate la informațiile înregistrate pe acesta și nu este lăsat accesibil acestor persoane (cu excepția cazurilor descrise la punctul 5.6);
- după transfer, fișierele sunt șterse imediat printr-o metodă de nerecuperare a datelor de pe suport convenită cu Serviciul protectie corporativa.

5.3. Mijloacele de stocare computerizate amovibile pentru informațiile confidențiale, trasabilitatea și distrugerea acestora trebuie înregistrate în conformitate cu actul normativ local care reglementează gestionarea informațiilor confidențiale.

5.4. Pentru a se evita furturile, înlocuirea, copierea sau infectarea mediilor externe de stocare utilizate de lucrători pentru a îndeplini sarcinile de producție, indiferent de prezența informațiilor confidențiale, acestea trebuie sa fie depozitate intr-un dulap sau intr-o incapere cu posibilitate de limitare acces. Indiferent de prezența informațiilor

confidențiale in acestea, mediile externe de stocare utilizate de lucrători pentru a îndeplini sarcinile de serviciu, pentru a evita lăsarea lor nesupravegheată și furturile, înlocuirea, copierea sau infectarea acestora, trebuie puse de către angajati într-un dulap ce se incuie sau sa se predea într-o încăpere care se incuie.

5.5. Pe mediile furnizate de PLK, precum și pe mediile personale care, în caz de pierdere sau furt, pot fi asociate cu societatea PETROTEL-LUKOIL, este interzisă înregistrarea și stocarea fișierelor care încalcă restricțiile legale și etica corporativă.

5.6. Transferul mediilor de stocare legate de activitățile de serviciu prin serviciile de transport / livrare ale terților ar trebui să se efectueze în containere care împiedică familiarizarea cu informațiile stocate, fără a afecta integritatea pachetului.

5.7. Este interzisă conectarea la echipamentele organizațiilor din PLK și la echipamentul personal autorizat pentru utilizare în activitățile de serviciu, a suporturilor media transmise sau lăsate de o persoană necunoscută.

5.8. Luând în considerare probabilitatea defectarii echipamentelor și mediilor de stocare, angajatii sunt obligați ca periodic să copieze informații de pe acestea, pierderile sau pagubele acestora putând dăuna sicietatii PETROTEL-LUKOIL, pe resurse de rețea a cărei locație poate fi solicitată de la Serviciul Tehnic.

5.9. În cazul întreruperii utilizării suportului (defectare, predarea la depozit, transferul la reparații, transferul spre folosirea de catre un alt angajat), angajatul este obligat să stearga de pe acesta toate informațiile referitoare la activitatea de serviciu și, dacă este imposibil din punct de vedere tehnic, să il predea Serviciului protectie corporativa pentru eliminare.

5.10. In cazul desfacerii contractului de munca, angajatul va preda suportul sefului sau direct.

6. Conturi

Este interzis lucrul de pe contul altcuiva, cu excepția înlocuirii unui alt angajat în timpul concediului acestuia (cu excepția concediului de crestere si ingrijire), concediului medical sau a trimiterii in delegatie a persoanei care a fost înlocuită, pe baza unei avizari (pe hârtie sau prin e-mail) din partea sefilor direcți ai acestor angajați. Răspunderea pentru utilizarea neautorizată a contului revine conducătorului angajatului care este înlocuit.

7. Retele de calculatoare corporative si resurse informationale

7.1. Conectarea echipamentelor la rețelele corporative prin cablu ale PLK și reconectarea acestora între prizele retelelor corporative prin cablu trebuie efectuata numai de către personalul tehnic autorizat al Serviciului de asistență tehnică, in urma solicitarii.

7.2. Conectarea wireless la rețelele corporative ale PLK, precum și conexiunea la distanță prin intermediul rețelelor altor operatori, sunt furnizate angajaților în

conformitate cu procedura stabilită în organizație, așa cum este stabilită de catre Serviciul protectie corporativă.

7.3. Accesul la resursele informaționale este oferit angajaților la cererea conducătorilor compartimentelor în conformitate cu acte normative locale ale organizației care deține resursele informaționale și în absența unor astfel de acte, în conformitate cu acte normative locale ale organizației care administreaza resursele informaționale.

7.4. In timpul utilizarii rețelelor corporative ale societatii PETROTEL-LUKOIL, se interzice angajaților:

- sa încerce să acceseze rețelele corporative ale organizațiilor din cadrul Grupului LUKOIL, resursele și serviciile de informații ale acestora, dacă acest acces nu a fost acordat angajatului in conformitate cu procedura in vigoare;
- sa utilizeze sau sa încerce să utilizeze dispozitivele disponibile în rețeaua corporativă, dacă accesul la acestea nu a fost organizat de un angajat al Serviciului de asistență tehnică;
- sa posteze pe resurse informaționale ale PLK sau în orice alt mod sa furnizeze in rețeaua comuna de acces, materiale care încalcă restricțiile legale și etica corporativă;
- crearea de resurse informationale fără autorizare (inclusiv foldere generale, secțiuni portal, servere web) sau servicii de rețea (servere de nume, servere proxy, puncte de acces, rețele de piraterie și etc.
- să utilizeze software fără permisiune; concepute pentru a căuta resurse de rețea sau vulnerabilități în ele (scanere de rețea), a asculta traficul de rețea (sniffers), controlul dispozitivului de la distanță prin rețea;
- să exploateze în mod intenționat vulnerabilitățile dispozitivelor de rețea, ale serviciilor și ale resurselor informaționale, precum și să verifice în mod independent existența unor astfel de vulnerabilități.

8. Regulile utilizarii postei electronice

8.1. Conturile din sistemul de e-mail corporate și alte sisteme de mesagerie electronică corporativă sunt furnizate angajaților numai pentru îndeplinirea sarcinilor de serviciu prevăzute în fișele de post.

8.2. Angajaților li se interzice să trimită mesaje care conțin informații confidențiale (inclusiv informații referitoare la activitățile organizațiilor din cadrul grupului LUKOIL care nu au o valoare comercială deliberată din cauza necunoștinței lor față de terți, dar care ar putea avea un impact negativ asupra activităților organizațiilor de grup LUKOIL"), catre sisteme necorporative fara un aviz din partea Serviciului protectie corporativă, cu excepția acelor sistemelor a căror utilizare este inclusă ca îndatorie de serviciu al angajatilor.

8.3. Pe dispozitivele staționare și mobile care aparțin PLK, inregistrarile în sistemele electronice terțe pot fi utilizate numai de comun acord cu Serviciul protective corporativă.

8.4. Este interzisă stabilirea unei redirecționări automate între conturi în sistemele de mesagerie electronică corporativă și sistemele de mesagerie electronică ale unor terțe părți.

8.5. Comunicațiile prin intermediul sistemelor de mesagerie electronică corporativă, precum și prin intermediul sistemelor de mesagerie electronică terță parte utilizate în coordonare cu departamentul de securitate corporativă ar trebui să fie efectuate în conformitate cu legile și reglementările locale care reglementeaza etica corporativă.

8.6. Atunci când se utilizează sisteme de mesagerie electronică care funcționează cu un microfon sau o cameră foto, angajații trebuie să se asigure că informațiile care nu sunt legate de o anumită sesiune de comunicare stabilită nu sunt transmise prin ele.

8.7. La transmiterea unui mesaj pe poștă electronică, angajatul este obligat să verifice dacă adresele destinatarilor sunt specificate corect, iar în cazul furnizării de informații confidențiale aparținând societatii PETROTEL-LUKOIL sau reprezentantilor imputerniciti ai sai - în absența printre persoanelor și organizațiilor ce nu au conventie sau contracte in vigoare de confidențialitate, ce contin clause de confidentialitate.

8.8. La transmiterea informațiilor confidențiale unui destinatar care nu se află în același complex de clădiri administrative, angajatul trebuie să clarifice prezența unui canal de transmisie securizat de e-mail. În lipsa unui canal securizat, angajatul trebuie să utilizeze instrumentele de protecție criptografice disponibile în organizație și pe partea destinatarului, în caz de absență, să trimită informații confidențiale sub forma unei arhive de fișiere protejate printr-o parolă, în conformitate cu cerințele privind protecția prin parolă.

8.9. Este interzisă transmiterea informațiilor confidențiale ale societatii PETROTEL-LUKOIL către adrese poștale personale ne-corporative postate pe serviciile poștale publice.

8.10. Este interzis să transmiteti mesaje electronice al căror conținut încalcă restricțiile legale și reglementările locale care reglementeaza etica corporativă.

8.11. Este interzisă transmiterea e-mailuri ale căror semnături conțin adrese poștale ne corporative, linkuri personale sau inregistrari in retele sociale.

8.12. Semnatura către e-mailul transmis se recomandă sa fie insotita de un text, care sa atraga atentia destinatarului că distribuirea ulterioară a informațiilor conținute in mesajul respectiv nu ar trebui să fie făcută de acesta fără autorizarea expeditorului.

8.13. Transmiterea neautorizată a mesajelor publicitare electronice este interzisă.

8.14. Este interzisă transmiterea de e-mailuri catre 100 sau mai multor destinatari, fără a contacta mai întâi Serviciul de asistență tehnică.

8.15. Este interzis să deschideți e-mailurile primite și fișierele atașate, precum și să urmați linkurile acestora fără a avea încredere în autenticitatea și siguranta expeditorului sau dacă mesajul pare neobișnuit pentru expeditorul specificat în acesta.

8.16. În cazul în care se primesc mesaje publicitare nedorite sau mesaje suspecte care conțin semne de fraudă sau încercări de a virusa calculatorul (fișiere atașate,

linkuri către resurse terțe ne-corporative etc.), angajatul este obligat să contacteze serviciul tehnic.

8.17. Pentru a primi instrucțiuni de lucrul cu filtrele spam care recunosc mesajele de e-mail nedorite și împiedică furnizarea acestora, angajatul trebuie să contacteze Serviciul de asistență tehnică.

9. Protecția parolei

9.1. Utilizarea parolelor personale care sunt greu de ghicit, selectat și păstrarea secretului de ceilalți este un mijloc esențial de protecție împotriva accesului neautorizat la resursele informaționale și a mijloacelor de procesare a acestora.

9.2. Angajații sunt obligați să-și schimbe imediat parolele atunci când își utilizează pentru prima dată contul, când resetează o parolă uitată atunci când suspectează că parola a fost compromisă și după trei luni de la modificarea parolei anterioare.

9.3. Atunci când creați o combinație de parole, angajații trebuie să îndeplinească următoarele cerințe:

- lungimea parola de cel puțin 8 caractere;
- parola include litere mari și mici, cifre și caractere speciale (<, >, =, *, #, $, %, ?, & etc.);
- parola nu conține o succesiune simplă de caractere (“Qwerty”, “AABbCc” etc.), informații personale (data nașterii copilului, marca automobilului, numărul de telefon de la serviciu etc.) sau cuvânt logic din dicționare;
- parola nu este formată din algoritmul simplu anterior (de exemplu, «abecedar1» «abecedar123»);
- parola nu coincide, cu utilizarea acesteia de catre angajat în alte inregistrari, inclusiv în viața cotidiană și în rețelele sociale.

9.4. Este interzisă divulgarea parolelor altor persoane, cu excepția cazului în care parola se transmite inlocuitorului de drept pe perioada de concediu (cu excepția concediului de ingrijire a copilului), boală sau deplasarea titularului prin aprobarea scrisa (pe hârtie sau prin e-mail). După revenire, angajatul care a transmis parola este obligat să schimbe imediat parola de utilizare.

9.5. Este interzisă introducerea parolelor în câmpul vizual al altor persoane, precum și în cazul în care formularul de solicitare a unei parole este diferit de cel obișnuit.

9.6. Este interzisă salvarea parolelor în fișiere sau utilizarea opțiunii de reținere automată a parolei în memoria dispozitivului.

9.7. Atunci când se înregistrează parola pe suport material, toate regulile stabilite pentru gestionarea informațiilor confidențiale ar trebui să fie aplicate celor din urmă.

9.8. Este interzisă luarea de măsuri pentru obținerea și utilizarea parolelor altor persoane.

9.9. Resetarea parolelor se realizeaza doar pe baza cererilor formalizate si aprobate ierarhic, prin Serviciului Tehnic IT. În cazuri excepționale, se va contacta Serviciul protectie corporativa.

9.10. În toate cazurile de compromitere a parolei, precum și la primirea notificarii de a comunica parola, angajații trebuie să acționeze în conformitate cu punctul 2.4, deoarece situațiile mentionate sunt incidente ale securitatii informaționale .

9.11. În cazurile permise de transferare a unui fișier arhivat cu o parolă unei alte persoane, parola pentru deschiderea acestuia trebuie trimisă folosind un alt canal de comunicare.

10. Protecție împotriva codului rău intenționat (malware)

10.1. Codul rău intenționat poate fi un fișier separat, inclusiv deghizat ca document, comandă rapidă, fișier multimedia sau încorporată în corpul unui alt program, document, fișier multimedia, e-mail sau pagină web.

10.2. Pericolul declansarii unui cod rău intenționat pe un dispozitiv electronic se datorează posibilei sale acțiuni neautorizate, cum ar fi:

- scurgere, distrugere sau deteriorare, inclusiv fără posibilitatea de recuperare a datelor stocate pe acesta;
- furtul de parole și coduri introduse pentru a accesa sisteme informaționale;
- infectarea suporturilor de date si unităților detașabile in timpul conectarii;
- trimiterea de mesaje electronice fără cunoștințele utilizatorului;
- posibilitatea de control ascuns dispozitivele la distanță, interceptarea imaginii afișate, activarea microfoanelor, a camerelor video și a interfețelor de rețea disponibile pe dispozitiv;
- organizarea atacurilor asupra altor noduri și a infrastructurii rețelelor la care se face legătura;
- substituirea adreselor sistemelor informatice accesate prin rețea.

10.3. Angajaților nu li se permite să elimine, să dezactiveze sau să reconfigureze software-ul antivirus instalat pe dispozitivele staționare și mobile ale societatii PETROTEL-LUKOIL sau premise de Serviciul protectie corporativa pentru utilizarea pe dispozitive personale permise pentru a fi utilizate în activități de serviciu.

10.4. În cazul în care pictograma care indică funcționarea software-ului anti-virus dispare sau se afișează notificări care semnalizează că funcționarea normală a fost întreruptă (expirarea licenței, depășita, componentele de protecție sunt dezactivate), precum și comportamentul atipic al aparatului (deschiderea și închiderea spontană a ferestrelor, redarea sunetelor, mișcarea pointerului mouse-ului, angajații ar trebui să contacteze imediat Serviciul de asistență tehnică.

10.5. Când primiți un mesaj pe ecran din software-ul antivirus care anunta ca fisierul infectat a fost mutat în carantină și dacă este nevoie să continuați să utilizați acest fișier, angajații ar trebui să contacteze serviciul de asistență tehnică.

10.6. Datorită posibilității ca un răufăcător să folosească un cod rău intenționat necunoscut dezvoltatorilor de software antivirus la momentul emiterii ultimei baze de date, este interzisă deschiderea fișierelor și a mesajelor e-mail din surse necunoscute, accesarea resurselor Internet îndoielnice, utilizarea unui mediu amovibil trimis sau lăsat de o persoană necunoscută.

11. Internet și rețele

11.1. Acces la Internet din rețele de calculatoare corporative, inclusiv fără fir, este furnizată angajaților în conformitate cu procedura aplicată în cadrul organizației și este destinată exclusiv îndeplinirii sarcinilor de serviciu prevăzute în fișele de post.

11.2. Securitatea privind activitatea pe Internet din rețeaua de computere este asigurată prin utilizarea instrumentelor de protecție centralizate, inclusiv servere terminale, firewall-uri, sisteme de prevenire a intruziunilor, sisteme de monitorizare și filtrare a traficului, gateway-uri anti-virus etc.

11.3. Conectarea dispozitivelor mobile aparținând societatii PETROTEL-LUKOIL și dispozitivele personale permise pentru a fi utilizate în activități de serviciu prin intermediul rețelelor altor operatori ar trebui să fie conectate de angajați, în măsura minimă necesară, ținând cont de riscurile semnificativ crescute:

- primirea de conținut rău intenționat;
- interceptarea traficului de către alți abonați ai rețelei utilizate;
- atacuri asupra dispozitivului de la alți abonați la Internet și rețeaua utilizată;
- substituirea adreselor site-urilor vizitate și a redirecționărilor utilizatorilor către site-uri false;
- crearea comenzilor false pentru a introduce parole, coduri și altele informații de autentificare;
- înregistrări ale sesiunii de comunicare a utilizatorului și statistici ale conexiunilor acestuia.

11.4. La accesarea Internetului din rețelele de calculatoare corporative, folosirea Internetului și rețelelor de utilizare comuna de la dispositivele mobile care in caz de pierdere sau accesarea acestora de la distanta de catre persoane neautorizate si pot fi asociate cu societatea PETROTEL-LUKOIL, angajatiilor li se interzice:

- descărcarea de pe Internet a aplicatiilor, cu excepția actualizărilor și completărilor necesare pentru programele instalate de Serviciul de asistență tehnică sau de catre Serviciul Protectie corporativa distribuite de producător;
- să primească de pe Internet programe software, material grafice, multimedia și texte care încalcă restricțiile legale și etica corporativă;
- sa distribuie neautorizat și să posteze date, conținând informații confidențiale (inclusiv informații referitoare la activitățile organizațiilor din cadrul grupului LUKOIL care nu au o valoare comercială deliberată datorită necunoscutului lor unor terțe părți, dar care ar putea avea un impact negativ asupra activităților organizațiilor din cadrul grupului LUKOIL);

- încercarea de a obține acces neautorizat la resursele informaționale ale internetului, la atacurile asupra site-urilor Internet și la alți abonați ai rețelei utilizate;
- încercarea de a ocoli metodele de conectare si mijloacele de protecție furnizate sau prescrise pentru utilizare.

12. Serviciul Cloud

12.1. Serviciul Cloud - serviciu bazat pe tehnologie distribuită de procesare a datelor pentru a oferi utilizatorului accesul la puterea de calcul prin Internet sau într-o rețea locală. Cele mai populare exemple sunt:

- servicii de partajare de fișiere (de exemplu, Dropbox, Yandex.Disk, Google Drive etc.);
- rețele sociale cu capacitatea de a descărca fișiere;
- site-uri web pentru redactarea documentelor de diverse formate sau pentru prelucrarea fotografiilor și videoclipurilor;
- servicii de sincronizare a datelor, note, contacte.

12.2. Angajaților li se interzice să posteze în serviciile cloud informații legate de activitățile de serviciu sau să organizeze accesul la serviciile cloud de la echipamentul societatii PETROTEL-LUKOIL sau din dispozitive personale permise de compartimentul de securitate corporativă pentru utilizarea în activități de serviciu. Excepție fac serviciile corporative sau serviciile cloud incluse în Lista de software și hardware obligatorie și recomandate pentru utilizarea în cadrul organizațiilor din grupul LUKOIL.

12.3. Având în vedere posibila lipsă a securității serviciilor cloud ale terților, angajații care utilizează astfel de servicii în scopuri personale ce nu tin de activitatea de serviciu nu li se recomandă să posteze date cu caracter personal și informații personale (de exemplu, copii scanate ale pașapoartelor și alte documente, numere de cont bancare etc.).

13. Protectia datelor cu caracter personal (GDPR)

PETROTEL-LUKOIL își ia angajamentul față de clienții săi și alte persoane care îi furnizează date cu caracter personal că va asigura confidențialitatea și securitatea datelor cu caracter personal în concordanță cu dispozițiile legale aplicabile în acest domeniu.

În îndeplinirea atribuțiilor de zi cu zi, atunci când este necesar, angajații PLK prelucrează date aparținând clienților persoane fizice, reprezentanților legali ai clienților persoane juridice și ai prestatorilor de servicii/utilități cu care PLK a încheiat relații contractuale etc.

Angajații care au acces la datele cu caracter personal trebuie să respecte următorele obligații principale:

13.1. Să prelucreze date cu caracter personal şi să acceseze documente / fişiere ce conţin date cu caracter personal doar dacă este necesar şi numai pentru îndeplinirea atribuţiilor specifice de serviciu;

13.2. Să nu acceseze mai multe informaţii decât este strict necesar pentru îndeplinirea sarcinilor de serviciu;

13.3. Să utilizeze parole pentru acest acces (conform capitol 9), parole ce au minimum opt caractere şi conţin cel puţin o literă mare şi cel puţin o cifră sau un simbol. Parolele trebuie schimbate cel puţin o dată la 3 luni. Angajaţii trebuie să îşi protejeze în permanenţă parolele şi să nu le comunice la nici o persoană, din cadrul PETROTEL-LUKOIL sau din afara organizaţiei;

13.4. Să blocheze ecranul computerelor şi terminalelor de acces atunci când se îndepărtează de ele (de ex., când pleacă într-o întâlnire, în pauza de masă, etc.);

13.5. Să nu lase laptopurile / echipamentele portabile / dosarele conţinând date cu caracter personal nesupravegheate şi să nu ia acasă registre conţinând date cu caracter personal.

13.6. Să nu printeze documente sau fişiere ce conţin date cu caracter personal decât atunci când este strict necesar în contexul realizării atribuţiilor de serviciu;

13.7. Să lase biroul curat la sfârşitul programului de lucru, precum şi în momentele în care lipsesc de la birou o durată mai lungă de timp (de ex., când pleacă în concediu);

13.8. Să respecte orice alte obligaţii stabilite de PETROTEL-LUKOIL prin proceduri interne şi instrucţiuni de lucru în scopul protejării datelor cu caracter personal.

14. Restrictii legislative si normele eticii corporative

14.1. Se interzice incarcarea, pastrarea, publicarea, difuzarea si acordarea accesului sau utilizarea in orice fel a informatiei, care incalca normele etice si standardele general valabile, si inclusiv contine scene de comportament violent fata de animale, amenintari, discrediteaza sau insulta alte persoane, contine limbaj vulgar si injuraturi.

14.2. Se interzice incarcarea, pastrarea, publicarea, difuzarea si acordarea accesului sau utilizarea in orice fel a informatiei, care incalca cerintele legislatiei romane si internationale, inclusiv:

- informatii confidenţiale a caror divulgare nu este autorizata de proprietar;
- date cu caracter personal, informatii despre viata privata, secrete personale sau familiale ale subiectilor care nu si-au dat consimtamantul pentru prelucrarea lor;
- rezultatele proprietatii intelectuale ale altcuiva, daca folosirea acestora incalca drepturile si interesele legitime ale titularilor de drepturi si ale altor persoane;
- virusi de calculator, fisiere malware, alte continuturi active, destinate accesului neautorizat la informatiile din calculator;
- orice imagini si texte pornografice, scene de natura sexuala;

- informații privind modurile, metodele de elaborare, fabricare a si utilizarea substantelor narcotice, substantelor psihotrope si precursorii acestora, locurile de achizitie a acestor mijloace, precum si metodele si locurile de cultivare a plantelor narcotice;
- informatii despre metodele de sinucidere, orice instigare la comiterea ei;
- informații care promoveaza si / sau contribuie la instigarea la ura rasiala, religioasa, etnica sau vrăjmasie;
- defaimare, adica informatie falsa in cunoștință de cauză, discreditarea onoarei și demnității unei alte persoane sau subminarea reputatiei sale;
- materiale extremiste, inclusiv ce propaga fascismul sau o ideologie a superioritatii rasiale, de schimbare violenta a fundamentelor ordinii constitutionale si incalcarea integritatii statului roman, justificarea terorismului si alte informatii a caror difuzare este restrictionata sau interzisa prin lege.

14.3. Este interzisa crearea, descarcarea, stocarea, copierea, transmiterea, distribuirea, furnizarea accesului sau utilizarea in orice alt fel *a oricaror informatii* care incalca Codul de etica in afaceri LUKOIL si / sau Regulile culturii corporative ale societatilor din cadrul grupului LUKOIL.

14.4. Nerespectarea restrictiilor mentionate poate duce la incalcarea normelor legislatiei in vigoare, a actelor normative locale a societatii PETROTEL-LUKOIL, ceea ce poate duce ulterior la atragerea angajatilor PLK la responsabilitatea prevazuta de lege.

15. Asistenta tehnica

15.1. Asistenta tehnica a calculatoarelor si a echipamentului de birou se efectuează in scopul remedierii neconformitatilor, instalarii si configurarii software-ului si a echipamentului si se efectueaza la cererea angajatului catre Serviciul de asistenta tehnica.

15.2. Asitenta tehnica locala se desfasoara la locul de munca al angajatului in prezenta sa. Daca este necesara scoaterea dispozitivului sau a partii sale din birou, angajatul are dreptul sa fie prezent in timpul efectuarii lucrarilor ulterioare.

15.3. Inainte de a transmite mediile de stocare, inclusiv cele din componenta dispozitivelor, pentru reparatiile efectuate de specialisti, angajatul este obligat sa stearga informatiile confidentiale din acestea, acționand conform instructiunilor Serviciului de Asistenta Tehnica.

15.4. Asistenta tehnica la distanta este utilizata pentru a accelera procesarea cererilor si este efectuata de la locul de munca al unui specialist autorizat sa efectueze tipul corespunzator de lucrari.

15.5. Sesiunea de mentenanta tehnica la distanta este posibila numai dupa ce angajatul a confirmat cererea pentru conexiunea la distanta, care este afisata pe ecran dupa aprobarea prealabila a timpului de incepere a lucrarilor.

15.6. Inainte de a permite o conexiune la distanta, angajatul trebuie sa-si inchida toate fisierele de lucru, precum si ferestrele aplicatiilor utilizate.

15.7. Angajatul poate vedea toate actiunile efectuate in timpul asistentei tehnice la distanta (deplasarea mouse-ului, copierea fisierelor, deschiderea ferestrelor etc.) si daca este necesar, sa intrerupa sesiuniea de asistenta la distanta.

15.8. Angajatul are dreptul sa intrerupa sesiunea de asistenta tehnica la distanta in urmatoarele cazuri:

-efectuarea unor actiuni suspecte de catre specialistul tehnic care nu au legatura cu rezolvarea problemei;

-nevoia de a pararsi de urgenta locul de munca;

-depasirea semnificativa a duratei lucrarilor convenite.

16. Explicarea modalitatii de indeplinire a Regulamentului

Dacă apar întrebări privind indeplinirea regulamentului, angajatii se pot adresa pentru clarificari persoanei responsabile de gestionarea incidentelor de securitate a informatiilor din cadrul societatii lor, desemnate pentru indeplinirea deciziei Nr. DAB 0056 din 21.02.2017.

Angajații Companiei PETROTEL-LUKOIL precum si firmelor terte, pot de asemenea, sa se adreseze catre Serviciul protectie corporativa pentru informatii cu privire la aplicarea Regulamentului.

PROCES VERBAL DE LUARE LA CUNOSTINTA SI PRELUCRARE

1. Tematica / Subiectele de prelucrare:

REGULAMENTUL PRIVIND ASIGURAREA SECURITATII INFORMATIONALE IN PETROTEL-LUKOIL S.A.

2. Responsabil instruire:

(numele si prenumele) (functia) (semnatura)

3. Subsemnatii am fost instruiti cu subiectele de mai sus, am inteles responsabilitatile ce ne revin si ne obligam sa le indeplinim:

Nr. Crt.	NUME/ PRENUME	Institutie/ Societate	SEMNATURA
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

4. Intocmit:

(numele si prenumele) (semnatura) (data)