Politica de securitate a resurselor informatice și de comunicații ale Universității Petrol-Gaze din Ploiești

Introducere	Regulamentele de Utilizare a Resurselor Informatice și de Comunicații sunt elaborate pentru a stabili un cadru corect, legal și eficient de utilizare a tehnologiei informației și comunicațiilor în cadrul Universității Petrol-Gaze din Ploiești. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea acestea au ca scop protejarea imaginii Universității și a investițiilor acesteia pentru dezvoltarea sistemul informatic și de comunicații.
Scop	În acord cu legislația în vigoare în România, Resursele Informatice și de Comunicații (RIC) sunt valori ale Universității Petrol-Gaze din Ploiești (UPG) care trebuie exploatate și administrate ca atare. Scopul acestor regulamente este acela de a asigura: 1. Stabilirea unor reguli corecte și eficiente pentru folosirea resurselor informatice și de comunicații în vederea sprijinirii proceselor didactice, administrative şi a cercetării științifice; 2. Protejarea imaginii Universității Petrol-Gaze din Ploiești; 3. Protejarea investițiilor Universității Petrol-Gaze din Ploiești aferente sistemului informatic și de comunicații propriu; 4. Protejarea proprietății intelectuale și a tuturor informațiilor stocate și transportate folosind Resursele Informatice și de Comunicații; 5. Educarea utilizatorilor resurselor informatice și de comunicații în ceea ce privește responsabilitățile asociate cu utilizarea acestora; 6. Compatibilitate cu regulamentele, statutul și atribuțiile stabilite pentru administrarea resurselor informatice și de comunicații.
Audiență	Regulamentele de utilizare a resurselor informatice și de comunicații ale UPG se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acesta. Următoarele entități și utilizatori sunt vizate/vizați în mod distinct de prevederile Politicii de securitate: - angajații UPG, cu contract de muncă pe perioadă determinată sau nedeterminată, care au acces la sistemul informatic și de comunicații al Universității; - colaboratorii UPG care au acces la Resursele Informatice și de Comunicații ale acesteia; - alte persoane, entități sau organizații care au acces la Resursele Informatice și de Comunicații ale UPG.
Scop	Politica de securitate a Resurselor Informatice și de Comunicații are ca scop asigurarea integrității, confidențialității și disponibilității informației. *Confidențialitatea* se referă la protecția datelor împotriva accesului neautorizat. Fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia și sub controlul UPG sunt proprietatea universității. Utilizatorul răspunde personal de confidențialitatea datelor

	încredințate prin procedurile de acces la Resursele Informatice și de Comunicații. *Integritatea* se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate. *Disponibilitatea* se asigură prin funcționarea continuă a tuturor componentelor Resurselor Informatice și de Comunicații. Diverse aplicații au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a Resurselor Informatice și de Comunicații. Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor și procedurilor de securitate. Acestea sunt obligatorii pentru toți utilizatorii Resurselor Informatice și de Comunicații.
Clasificarea Informațiilor	Clasificarea informațiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora cât și pentru a determina pierderile potențiale ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora. Pentru a asigura securitatea și integritatea informațiilor, acestea se împart în trei categorii principale: - Publice - Secrete - Strict Secrete Administratorul de Rețea și conducerile Departamentelor răspund de evaluarea periodică a schemei de clasificare a informațiilor. Toate informațiile gestionate de UPG trebuie să se regăsească în una din următoarele categorii: 1. Publice - Acestea sunt informațiile accesibile oricărui utilizator din interiorul sau exteriorul UPG. Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produc efecte asupra instituției sau aceste efecte sunt nesemnificative. Utilizatorii care furnizează aceste informații sunt responsabili de asigurarea integrității și disponibilității acestora în raport cu cerințele firmei. 2. Secrete - În această categorie se includ informațiile care datorită valorii economice nu trebuie făcute publice. Se includ aici și informațiile pe care UPG trebuie să le protejeze conform legislației în vigoare. Datorită valorii economice asociate, aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate şi distribuite în cadrul universității doar utilizatorilor autorizați. Exemple relevante: clauze contractuale, conturi si parole folosite pe serverele de contabilitate sau gestiune, conturi și parole pentru accesul la Sistemul Informatic Didactic (SID). 3. Strict Secrete - În această categorie se includ toate informațiile care datorită valorii economice nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date pot intra sub incidența Codului Civil, Penal sau Fiscal. Accesul la aceste informații va fi restricționat. Datele strict secrete nu pot fi copiate, distribuite sau șterse fără acordul scris al conducerii universității. Exemple relevante: cheile criptografice, conturi administrative de pe

	servere, date financiare, schițe pentru prototipuri, coduri sursă protejate.
Definiţii	*Resurse Informatice și de Comunicații (RIC):* toate dispozitivele de tipărire/imprimare, dispozitive de afișare, unități de stocare, și toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând servere, calculatoare personale, notebook-uri, calculatoare portabile, asistent digital personal (Personal Digital Assistant - PDA), pagere, sisteme de procesare distribuită, echipament de laborator conectat la rețea și controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, imprimante și alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele și datele care sunt proiectate, construite și menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afișa și transmite informația. *Utilizator:* O persoană, o aplicație automatizată sau proces autorizat de către UPG, în conformitate cu procedurile și regulamentele în vigoare, să folosească RIC. *Furnizor:* Persoană fizică/juridică care oferă bunuri sau servicii Universității Petrol-Gaze din Ploiești în baza unui contract comercial sau de colaborare. *Abuz de privilegii*: Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele şi/sau cu legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acțiunii respective.
Confidențialitate	1. Fișierele electronice create, trimise, primite sau stocate folosind Resursele Informatice și de Comunicații administrate sau în custodia și sub controlul UPG nu au caracter personal și pot fi accesate oricând de către personalul autorizat, fără înștiințarea utilizatorului. 2. În scopul administrării Resurselor Informatice și de Comunicații și pentru asigurarea securității acestora, personalul autorizat poate revizui sau utiliza orice informație stocată pe sau transportată prin sistemele Resurselor Informatice și de Comunicații în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor (de exemplu, dar fără a se limita la, numere de telefon formate sau sit-uri web vizitate, e-mailuri trimise sau primite). 3. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul UPG, orice incident de posibilă întrebuințare greșită sau încălcare a acestui regulament, prin contactarea personalului Departamentului Tehnologia Informației și Comunicații (DTIC). 4. Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele Universității. pentru care nu au autorizație sau consimțământ explicit. 6. Nici un utilizator al Resurselor Informatice și de Comunicații nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemelor ce compun Resursele Informatice şi de Comunicaţii. Această regulă se extinde şi după ce utilizatorul a încheiat relațiile cu UPG. 7. Confidențialitatea informațiilor transmise prin intermediul resurselor de

	comunicații ale terților nu poate fi asigurată. Pentru aceste situații, confidențialitatea și integritatea informațiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligați să se asigure că toate informațiile confidențiale ale UPG se transmit în așa fel încât să se asigure confidențialitatea și integritatea acestora.
Regulament de Utilizare Acceptabilă a RIC	1. Utilizatorii trebuie să anunțe *personalul autorizat DTIC* în cazul în care se observă orice problemă/breșă în sistemul de securitate a RIC cât și orice posibilă întrebuințare greșită sau încălcare a regulamentelor în vigoare. 2. Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și de comunicații și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea şi disponibilitatea informațiilor de orice tip în cadrul sistemului RIC al Universității Petrol-Gaze din Ploiești. 3. Utilizatorii nu trebuie să încerce să obțină acces la date sau programe din RIC pentru care nu au autorizație sau consimțământ explicit. 4. Utilizatorii nu trebuie să divulge sau să înstrăineze nume de conturi, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive și/sau informații similare utilizate în scopuri de autorizare a accesului și identificare. 5. Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright). 6. Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea *personalului autorizat DTIC*, cu excepția cazului în care acestea se găsesc pe lista programelor standard folosite în cadrul Universității. Această listă va fi întocmită de către DTIC împreună cu directorul/responsabilul fiecărui Departament și aprobată de către conducerea universității. 7. Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane; să degradeze performanțele RIC; să împiedice accesul unui utilizator autorizat la RIC; să obțină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente. 8. Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității RIC. De exemplu, utilizatorii din cadrul Universității nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente. 9. Resursele informatice ale UPG nu trebuie folosite pentru beneficiul personal. 10. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale care pot fi considerate ofensive, indecente sau obscene 11. Accesul la rețeaua Internet prin intermediul RIC se realizează doar în beneficiul universității și este monitorizat permanent. 12. Utilizatorii vor folosi, exclusiv, numele de domeniu *upg-ploiesti.ro* în toate activitățile desfășurate prin intermediul sau folosind sistemul RIC al Universității. Utilizarea denumirilor pentru calculatoare şi a adreselor de e-mail care nu au

	sufixul *upg-ploiesti.ro* sau *upg.local* este strict interzisă. 13. Fiecare utilizator este responsabil de modul în care utilizează resursele informatice puse la dispoziție; fiecare utilizator este direct responsabil pentru acțiunile care pot afecta securitatea informatică a UPG; 14. Nu este permisă transmiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva UPG Ploiești, sau prejudicierea, indiferent de formă, a intereselor universității. 15. Toate mesajele, fișierele și documentele – inclusiv mesajele sau fișierele personale – localizate în cadrul Resurselor Informatice și de Comunicații sunt proprietatea UPG și pot fi verificate și accesate, modificate sau șterse fără notificarea prealabilă de către personalul autorizat din aceasta. 16. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nu numai, mesagerie electronică, navigare Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare. 17. Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația și datele trebuie protejate fiind proprietatea UPG Ploiești. 18. Orice program comercial utilizat în cadrul RIC trebuie să fie însoțit de Licență care să specifice clar drepturile de utilizare și restricțiile produsului. Personalul trebuie să respecte prevederile Licențelor si nu este permisă copierea ilegală a programelor comerciale. *Personalul autorizat DTIC* își rezervă dreptul de a șterge orice produs fără Licență de pe orice sistem din cadrul RIC 19. *Personalul autorizat DTIC* își rezervă dreptul de a șterge, de pe orice sistem, orice program sau fișier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fișiere, dar nu limitate la: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), fișiere cu muzică (mp3, wav etc.), fișiere grafice (bmp, gif, jpg etc.), programe tip freeware şi shareware. 20. Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi. 21. Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activității pe care o desfășoară, astfel nu se vor folosi privilegii administrative pentru editarea documentelor sau pentru accesarea e-mailurilor. Accesul pe conturile privilegiate se realizează doar pentru îndeplinirea sarcinilor administrative care nu se pot realiza de pe celelalte conturi de utilizator. 22. Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al *Administratorului de rețea* şi trebuie să fie schimbată atunci când persoana care utilizează acest cont își schimbă locul de muncă. 23. Parolele pentru conturile cu acces privilegiat (drepturi de administrator, etc) se

vor depozita, sub semnătură, individual, în plicuri sigilate la Rectoratul Universității. Accesul la aceste date se va face doar în cazul indisponibilității deținătorului contului, în prezența Rectorului (sau a unui Prorector) și a unui reprezentat DTIC.

24. Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operațiuni cu caracter temporar. Acestea trebuie să îndeplinească următoarele condiții:

    - trebuie să fie autorizate;
    - trebuie create cu dată de expirare specifică;
    - orice cont va fi șters atunci când nu mai este necesar.

25. Măsurile de Securitate ale Resurselor Informatice nu trebuie să fie ocolite sau dezactivate utilizând conturi de acces privilegiat.
26. Fiecare Departament trebuie să permită *personalului DTIC* sau persoanelor autorizate accesul și folosirea mijloacelor de control în scopul monitorizării RIC în scopul protejării datelor și programelor împotriva întrebuințării greșite, în concordanță cu necesitățile stabilite de acestea.
27. DTIC trebuie să aprobe în scris conectarea dispozitivelor de calcul la RIC. Pentru fiecare sistem trebuie să existe o persoană care să răspundă de acestea, numele și datele de identificare ale acesteia se vor comunica *personalului autorizat DTIC*.
28. Conectarea sistemelor de calcul care nu sunt proprietatea Universității (laptop-uri personale ale angajaților, telefoane mobile cu WiFi, computere ale partenerilor și colaboratorilor) se face numai cu aprobarea în scris de către DTIC, la cererea utilizatorilor și cu recomandarea directorilor/responsabililor de Departament.
29. Accesul de la distanță la rețeaua Universității este strict interzis, cu excepția personalului autorizat în mod explicit pentru configurarea de la distanță. Acesta va accesa rețeaua doar prin echipamente securizate, prin canale de comunicații criptate aparținând unor Furnizori de Servicii Internet (ISP) agreați de UPG.
30. Utilizatorii nu au dreptul să extindă sau să retransmită serviciile de rețea pe nici o cale. Nu este permisă instalarea de conexiuni de rețea, fără autorizare scrisă din partea *DTIC*, indiferent de motiv. Este strict interzisă instalarea de telefoane, fax-uri, modemuri, routere, switchuri sau puncte de acces wireless în rețeaua Universității. Autorizarea se face la propunerea directorilor/responsabililor Departamentelor.
31. Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de rețea fără aprobarea *DTIC.*
32. Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de rețea, cabluri prize de rețea.
33. Serviciul de nume de domenii și administrarea adreselor IP sunt deservite exclusiv de către *DTIC.* Alocarea de adrese IP / nume de domenii se realizează numai de către personalul DTIC.

	34. Pentru a furniza o infrastructură de comunicații unitară cu posibilități de modernizare toate componentele acesteia sunt instalate de către *DTIC* sau de către furnizori avizați explicit de acesta. 35. Toate echipamentele, fără excepție, conectate la rețeaua de comunicații trebuie configurate conform specificațiilor furnizate de *personalul autorizat DTIC.* 36. Toate conectările dintre rețeaua de comunicații a Universității Petrol-Gaze din Ploiești și alte rețele de comunicații publice sau private, sunt responsabilitatea exclusivă a *personalului autorizat DTIC.* 37. Monitorizarea RIC se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice și a situațiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate vor urmări și înregistra: • Tipul traficului extern și conținutul acestuia • Tipul traficului intern și conținutul acestuia precum și echipamentele conectate la RIC. 38. În mod regulat se vor efectua verificări de către *personalul autorizat DTIC* pentru detectarea: • Parolelor care nu respectă cerințele de securitate; • Echipamentelor de rețea conectate neautorizat; • Serviciilor de rețea neautorizate; • Serverelor neautorizate; • Licențelor pentru sistemele de operare si programele instalate. 39. Parolele utilizate trebuie să respecte următoarele reguli: • Dimensiune de minim 8 caractere; • Trebuie să conțină cel puțin: ○ o literă mare ○ o literă mică ○ o cifră ○ un caracter special. 40. Parolele vor fi schimbate periodic (recomandat la fiecare 45 de zile). 41. Toți utilizatorii sistemului RIC, fără excepție, vor folosi adrese de e-mail din domeniul upg-ploiesti.ro 42. Următoarele activități sunt strict interzise: • Trimiterea de mesaje cu caracter de intimidare sau hărțuire; • Folosirea sistemului de mesagerie electronică în scopuri politice; • Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate; • Folosirea altei identități decât cea reală atunci când e transmit e-mailuri; • Trimiterea sau retrimiterea de e-mailuri în lanț (SPAM); • Trimiterea mesajelor nesolicitate către grupuri de persoane, cu excepția cazurilor în care aceste mesaje deservesc instituția. • Trimiterea mesajelor de dimensiuni mari (peste 10 MB). 43. Toate informațiile și datele confidențiale ale Universității Petrol-Gaze din Ploiești. transmise către alte rețele externe, trebuie să fie criptate.

	44. Toate activitățile utilizatorilor ce implică accesul și/sau folosirea RIC și serviciilor de e-mail pot fi oricând înregistrate și analizate. 45. Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că își spun opinia sau dau declarații în numele Universității Petrol-Gaze din Ploiești, cu excepția situațiilor în care aceștia sunt autorizați în mod corespunzător (implicit sau explicit) să acest lucru. Atunci când este cazul, se va include o declarație explicită prin care utilizatorul specifică faptul că nu reprezintă UPG. Un exemplu de declarație simplă este: "Părerile exprimate sunt personale, și nu reprezintă poziția oficială a Universității Petrol-Gaze din Ploiești.". 46. Utilizatorii nu trebuie să trimită, retrimită sau să primească informații confidențiale sau senzitive ce privesc Universitatea Petrol-Gaze din Ploiești, folosind conturi utilizator care nu sunt proprietatea firmei. Exemple de astfel de conturi sunt Hotmail, Yahoo, AOL mail sau adrese puse la dispoziție de alți Furnizori de Servicii de Internet. 47. Cumpărăturile de pe Internet, de pe domeniul upg-ploiesti.ro, care nu au legătură cu atribuțiile de serviciu sunt interzise. Cumpărăturile în interes de serviciu se vor supune regulilor de achiziție ale Universității Petrol-Gaze din Ploiești 48. Fișierele electronice se supun acelorași reguli de păstrare ce se aplică și altor documente și trebuie păstrate în conformitate cu regulile stabilite prin prezentul Regulament, prin regulamentele proprii fiecărui Departament și prin legislația în vigoare.
Măsuri Disciplinare	Încălcarea acestui regulament se sancționează prin măsuri disciplinare care pot include: 1. Rezilierea contractului de muncă în cazul angajaților; 2. Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor; 3. Interzicerea accesului la sistemul RIC. Toate acțiunile care contravin legilor vor fi raportate organelor competente.
Referințe	1. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt 2. ISO 17799 – Standard detaliat de securitate: 3. http://www.iso17799software.com/what.htm 4. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei. 5. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. 6. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 7. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică. 8. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.

	9. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică. 10. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal. 11. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 12. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. 13. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu. 14. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.
Versiune: 1.0.0 Aprobat: 20.04.2015 Efectiv: 01.05.2015	Autor: Ing. Emil PRICOP Aprobat: Prof. Dr. Ing. Mihai Pascu COLOJA Rector al Universității Petrol-Gaze din Ploiești