PLANUL DE SECURITATE CIBERNETICA

AL SISTEMULUI RESURSELOR INFORMATICE SI DE COMUNICATII

S.C. COMPANIA REGIONALA DE APA BACAU S.A.

Aprobat:	**Director General**: Doru CONSTANTIN	
	Ediția I	
	Intrat în vigoare la data de: **09.12.2024**	
Elaborat:	Negurita Gabriel	Adrian Oprisan

Capitolul 1. Dispoziţii generale

Art. 1. În acord cu prevederile prezentului regulament, Resursele Informatice şi de Comunicaţii administrate de către Compartimentul Gestionarea Sistemului Informatic si Serviciul Tehnic (SCADA) sunt bunuri/active strategice ale S.C. COMPANIA REGIONALA DE APA BACAU S.A.;

Art. 2. Documentele interne de reglementare a utilizării Resurselor Informatice şi de Comunicaţii sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în cadrul S.C. COMPANIA REGIONALA DE APA BACAU S.A.;

Art. 3. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea, acestea vizează protejarea imaginii companiei şi a investiţiilor acesteia pentru dezvoltarea sistemului informatic şi de comunicaţii;

Art. 4. Reţeaua informatică a S.C. CRAB S.A. sprijină procesul de business prin mijloacele de comunicare şi serviciile specifice oferite de reţelele de calculatoare;

Art. 5. Compromiterea securităţii acestor resurse poate afecta capacitatea companiei de a oferi servicii informatice şi de comunicaţii, poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilităţii companiei în faţa partenerilor săi. Prin urmare, prezentul regulament este motivat tehnic de necesitatea menţinerii în funcţiune, în condiţii de securitate, a reţelei S.C. CRAB S.A., precum şi de necesitatea dezvoltării normale a unei resurse de informare;

Art. 5. Scopul urmărit de politica de securitate este acela de asigurare a integrităţii, confidenţialităţii şi disponibilităţii informaţiei, precum şi stabilirea cadrului necesar pentru elaborarea regulilor şi procedurilor de securitate;

(1) *Confidenţialitatea* se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul S.C. CRAB S.A. sunt proprietatea companiei în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la Resursele Informatice şi de Comunicaţii;

(2) *Integritatea* se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate;

(3) *Disponibilitatea* se asigură prin funcţionarea continuă a tuturor componentelor Resurselor Informatice şi de Comunicaţii. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a Resurselor Informatice şi de Comunicaţii.

Capitolul 2. Documente de referinţă

Art. 6. Legislaţie primară

(1) Orice activitate care se desfăşoară prin intermediul reţelei S.C. CRAB S.A. trebuie să respecte legislaţia în vigoare (internă şi internaţională):
- Legea nr. 8/1996, privind dreptul de autor şi drepturile conexe;

- HG 58/1998 – pentru aprobarea Strategiei naţionale de informatizare şi implementare în ritm accelerat a societăţii informaţionale şi a Programului de acţiuni privind utilizarea pe scară largă şi dezvoltarea sectorului tehnologiilor informaţiei în România;
- Ordonanţa de Guvern nr. 124/200 – pentru completarea cadrului juridic privind dreptul de autor şi drepturile conexe, prin adoptarea de măsuri pentru combaterea pirateriei în domeniile audio şi video, precum şi a programelor pentru calculator;
- Legea nr. 544/2001 privind liberul acces la informaţiile de interes public;
- Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
- Convenţia privind Criminalitatea Informatică a Consiliului Europei;
- Declaraţia privind libertatea comunicării pe Internet a Consiliului Europei;
- Legea NIS 362/2018.

(2) Legislaţia primară va fi actualizată cu modificările şi completările ulterioare, dar şi cu alte acte normative relevante în domeniul securităţii informatice.

Art. 7. Reglementări interne
(1) Regulamentele şi procedurile în vigoare în cadrul S.C. CRAB S.A.;

Capitolul 3. Definiţii

Art. 8. *LAN* = reţeaua internă de calculatoare, *WAN* = reteaua externa de calculatoare;

Art. 9. *Cont* = o entitate specificată printr-un identificator şi/sau parolă pentru accesul la sistemul de comunicaţie şi/sau la o resursă de calcul;

Art. 10. *Resurse IT* = toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare, şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframeuri, servere, calculatoare personale, calculatoare-agendă (*notebookuri*, *laptop*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.

Art. 11. *Inginerul de sistem/Administratorul de reţea* este şi *Administratorul Resurselor Informatice si de Comunicare* = persoana responsabilă la nivelul companiei cu administrarea Resurselor IT;

Art. 12. *Utilizator* = o persoană, o aplicaţie automatizată sau proces utilizator autorizat de către, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele IT;

Art. 13. *Abuz de privilegii* = orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele S.C. CRAB S.A. şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.

Art. 14. *Furnizor*: Persoană fizică/juridică care oferă bunuri sau servicii S.C. CRAB S.A. în baza unui contract comercial sau de colaborare.

Capitolul 4.

4.1. Politica de securitate

Art. 15. Politica de securitate este alcătuită astfel încât să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice publice, să stabilească practici prudente şi acceptabile privind utilizarea Resurselor Informatice şi de Comunicaţii ale S.C. CRAB S.A. şi să instruiască utilizatorii care au dreptul de folosire a Resurselor Informatice şi de Comunicaţii privind responsabilităţile asociate unei astfel de utilizări.

Art. 16. Clasificarea informaţiilor din punct de vedere al securităţii şi integrităţii informaţiilor:

(1) Informaţii Publice (neetichetate) - acestea sunt informaţii accesibile oricărui utilizator din interiorul sau exteriorul companiei. Exemplu de astfel de date sunt cele de pe site-urile Web sau informaţiile de presă. Publicarea informaţiilor nu poate dăuna organizaţiei în niciun fel.

(2) Informaţii de Uz Intern - Accesul neautorizat la aceste informaţii poate cauza daune minore şi/sau deranj organizaţiei. Informaţiile sunt disponibile tuturor angajaţilor şi unor anumiţi terţi.

(3) Informaţii Restrictionate - Accesul neautorizat la informaţii poate dăuna în mod considerabil afacerii şi/sau reputaţiei organizaţiei. Informaţiile sunt disponibile doar unui anumit grup de angajaţi şi terţi autorizaţi.

(4) Informaţii Confidentiale - Accesul neautorizat la informaţii poate cauza daune catastrofale (ireparabile) afacerii şi/sau reputaţiei organizaţiei. Informaţiile sunt disponibile doar persoanelor din cadrul organizaţiei. Ex: parole la servere importante, chei de criptare etc.

4.2. Audienţă

Art. 17. Politica de securitate a resurselor IT în S.C. CRAB S.A. se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a instituţiei.

Art. 18. Următoarele entităţi şi utilizatori sunt vizaţi în mod distinct de prevederile Politicii:

(1) Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;

(2) Colaboratorii S.C. CRAB S.A. care au acces la resursele IT;

(3) Furnizorii S.C. CRAB S.A. care au acces la resursele IT;

(4) Alte persoane, entităţi sau organizaţii care au acces la resursele IT.

4.3. Atribuţii si obligaţii

Art. 19. Administratorii reţelelor din cadrul infrastructurii IT si SCADA, reprezentaţi prin Compartimentul Gestionarea Sistemului Informatic si Serviciul Tehnic, au următoarele atribuţii cu privire la Politicile de Securitate:

(1) Elaborează şi propune modificări ale Planului de Securitate;

(2) Elaborează şi propune pentru aprobare regulamentele şi procedurile de securitate;

(3) Tratarea incidentelor de securitate;

(4) Elaborează proceduri pentru identificarea utilizatorilor.

Art. 20. Atribuţiile utilizatorilor sunt:

(1) Să cunoasca şi să respecte prevederile Planului de Securitate;

(2) Să cunoască şi să respecte prevederile regulamentelor şi procedurilor de securitate;

(3) Să răspundă direct de securitatea şi conţinutul informaţiilor şi resursele informatice şi de comunicaţii încredinţate direct sau indirect.

Art. 21. Toți partenerii S.C. CRAB S.A. trebuie să accepte și să respecte aceste politici de securitate.

4.4. Confidențialitatea informațiilor

Art. 22. Fiecare utilizator este responsabil în mod direct de modul de utilizare a resurselor companiei;

Art. 23. Nu există nici o asigurare a confidenţialităţii datelor personale sau a accesului la informaţii, mesagerie electronică, navigare Web, acces la rețelele Wireless, transmisie fax-uri şi alte instrumente de conversaţie electronica in cazul utilizarii acestora in cadrul infrastructurii IT a SC CRAB SA. Utilizarea acestor instrumente de comunicaţie electronică poate fi monitorizată în scopul unor investigaţii sau al rezolvării unor plângeri în condiţiile legilor în vigoare.

Art. 24. Modul de acces la resursele companiei trebuie reglementat şi monitorizat împotriva întrebuințării greşite sau rău voite.

Art. 25. Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele sunt proprietatea companiei şi trebuie să fie protejate.

Art. 26 Compartimentul Gestionarea Sistemului Informatic si Serviciul Tehnic (SCADA) îşi rezervă dreptul de a şterge, de pe orice sistem orice program sau fişier ce nu are legătura cu scopul muncii respective, sau contravine politicilor companiei. De asemenea se poate suspenda functionarea oricărui echipament care poate afecta functionarea sistemelor din cadrul companiei;

Art. 27. Personalul autorizat poate revizui sau utiliza orice informaţie stocată sau transportată prin sistemele companiei în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor (cu titlu de exemplu nelimitativ: site-uri web vizitate, etc.).

Art. 28. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul S.C. CRAB S.A., orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament.

Art. 29. Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele companiei pentru care nu au autorizaţie sau consimţământ explicit;

Art. 30. Niciun utilizator al sistemelor din S.C. CRAB S.A. nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu compania;

Art. 31. Informaţiile publicate electronic de către S.C. CRAB S.A. pe site-ul propriu ***apabacau.ro***, respectiv ***apaserv.ro*** şi în subdomeniile acestuia sunt proprietatea companiei. Caracterul public al acestora reflectă faptul că ele sunt puse la dispoziţie de către S.C. CRAB S.A. în beneficiul comunităţii publice, în scop de informare asupra proiectelor şi a activităţii S.C. CRAB S.A.;

Art. 32. Informaţiile depuse pe site-urile publice ale S.C. CRAB S.A. aparţin companiei. Orice utilizare a informaţiilor de pe site-urile publice ale companiei de către persoane particulare sau organizaţii în alte scopuri decât cele în care au fost oferite, se face pe propria răspundere a acestora.

Capitolul 5.

5.1. Planul de securitate

Art. 33 Planul de securitate a S.C. CRAB S.A. impune dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau reguli specifice care să asigure integritatea, confidenţialitatea şi disponibilitatea informaţiei în utilizarea RIC;

Art. 34. Planul de securitate conţine regulile şi procedurile aplicabile în sistemul Resurselor Informatice şi de Comunicaţii ale S.C. CRAB S.A.;

Art. 35. Planul de securitate are ca scop principal protejarea utilizatorilor şi colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea, acesta are ca scop protejarea imaginii companiei şi a investiţiilor acesteia pentru dezvoltarea sistemului informatic şi de comunicaţii, protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate cu ajutorul Resurselor Informatice şi de Comunicaţii ale utilizatorilor autorizaţi: salariati, personal administrativ, colaboratori, etc;

Art. 36. Regulile au fost elaborate pentru fiecare activitate specifică domeniului şi au fost concepute în aşa fel încât fiecare să poată fi folosită cvasiindependent de celelalte;

Art. 37. Regulile şi procedurile din planul de securitate au rolul:

(1) de a fi corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţie în vederea sprijinirii procesului de business al companiei;

(2) de a fi compatibile cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

Art. 38. Regulile de utilizare a Resurselor Informatice şi de Comunicaţii ale S.C. CRAB S.A. se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la aceste resurse;

5.2. Procedee şi reglementări

Art. 39. Regulamentul privind accesul la reţelele LAN / WAN şi utilizarea aplicaţiilor software prevede următoarele reguli privind accesul la email:

(1) Orice parolă trebuie să fie complexă. Pentru parole se respectă Regulile privind parolele de acces de mai jos.

(2) Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces şi datele din acestea;

(3) Utilizatorii nu trebuie să trimită, retrimită sau să primească informaţii confidenţiale sau senzitive ce privesc compania, folosind conturi utilizator care nu sunt proprietatea companiei. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea): Hotmail, Yahoo mail, AOL mail, precum şi adrese de e-mail puse la dispoziţie de alţi Furnizori de Servicii Internet.

Art. 40. De asemenea, accesul la reţeaua intranet/internet şi utilizarea aplicaţiilor software, referitor la accesul la email, este interzis pentru:

(1) Trimiterea de mesaje cu caracter de intimidare sau hărţuire;

(2) Folosirea sistemului de mesagerie electronică în scopuri personale;

(3) Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;

(4) Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;

(5) Folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.

(6) Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia.

Art. 41. Compartimentul Gestionarea Sistemului Informatic asigură confidenţialitatea datelor personale sau a accesului la informaţii folosind poşta electronică sau alte instrumente de conversaţie electronică in limitele competentelor, a posibilităţilor tehnice existente şi a limitelor impuse de prevederile legale în vigoare.

5.3. Reglementari privind securitatea datelor

Art. 42. Securizarea serverelor se realizează prin următoarele reguli:

(1) Serverele trebuie să fie într-o locaţie cu acces securizat; accesul este restricţionat doar la personalul tehnic autorizat;

(2) Instalarea sistemului de operare dintr-o sursă aprobată;

(3) Setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;

(4) Dezactivarea sau schimbarea parolelor conturilor predefinite;

(5) Crearea şi utilizarea copiilor de siguranţă (backup).

Art. 43. Regulile privind parolele de acces sunt următoarele:

(1) Orice parolă ar trebui să fie complexă şi să aibă o lungime minimă de 8 caractere. O parolă complexă este un şir de caractere compus din litere minuscule, majuscule, cifre şi simboluri (%$#&^* ...);

(2) Nu folosiţi aceeaşi parolă pentru mai multe conturi;

(3) Dacă aveţi multe parole le puteţi scrie într-un fişier, însă criptaţi acel fişier şi asiguraţi-vă că nu-l veţi pierde. Evitaţi denumirea acelui fişier cu una explicită (ex. parolelemele.rar);

(4) Evitaţi să păstraţi parole în agende electronice, telefoane mobile;

(5) Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puţin o dată la 90 de zile;

(6) Aveţi grijă la facilitatea browser-elor de reţinere a parolelor (AutoFill, Remember password) cu atât mai mult atunci când calculatorul pe care lucraţi e folosit de mai multi utilizatori;

(7) Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice;

(8) Dacă se suspectează că o parolă a putut fi divulgată, aceasta trebuie schimbată imediat;

(9) Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ;

(10) Dispozitivele de calcul nu trebuie lăsate nesupravegheate, fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă;

Art. 44. Alte reglementări privind securitatea sunt cele care urmează, acestea se referă la activităţi interzise precum:

(1) Activităţi comerciale neautorizate;

(2) Trafic masiv de informaţii sau trafic de informaţii cu caracter frivol, obscen şi pornografic;

(3) Folosirea unor drepturi de acces la resurse pentru care nu sunt autorizaţi;

(4) Ştergerea sau alterarea datelor altor utilizatori;

(5) Tentativele de descoperire şi de folosire a parolelor altor utilizatori;

(6) Crearea sau folosirea de instrumente soft destinate spargerii sistemelor de securitate ale calculatoarelor;

(7) Provocarea deliberată de defectiuni hardware şi software;

(8) Perturbarea traficului reţelei companiei;

(9) Generarea de trafic necorespunzator companiei;

(10) Transferuri de materiale care contravin legilor drepturilor de autor (software pirat, filme, muzică, cărţi etc.);

(11) Generarea de spam;

(12) Flood (indiferent de natura acestuia), de exemplu: ping flood;

(13) Răspândirea de aplicaţii de tip virus, troieni, viermi, spyware sau altele;

(14) Folosirea de aplicaţii de tip key-logere;

(15) Modificarea adresei MAC a plăcii de reţea;

(16) Setările pentru IP şi DNS, altfel decât cu "Obtain an IP/DNS address automatically", fără autorizaţie din partea C.G.S.I.;

(17) Utilizarea de programe pentru scanarea reţelei, exploit-uri;

(18) Folosirea de software fără licenţă pe calculatoarele din companie sau conectate la reteaua companiei.

5.4. Reglementări/procedee administrare informaţii

Art. 45. Regulile specifice privind administrarea informaţiilor şi activităţi de mentenanţă sunt conţinute si elaborate în PROCEDURI NIS (PO-NIS).

Art. 46. Reguli de administrare a conturilor de email:

(1) Fiecare cont de email creat pe domeniul apabacau.ro trebuie să aibă asociate o cerere şi o aprobare corespunzătoare;

(2) Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces;

(3) Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat;

(4) Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Regulile privind Parolele de Acces;

(5) Numărul de mesaje din Inbox nu este limitat;

(6) Pentru păstrarea tuturor mesajelor primite este necesară, daca este posibil, instalarea unui client local de email (ex: Mozilla Thunderbird, Outlook Express etc.) pe calculatorul individual al fiecărui utilizator;

(7) Accesul la sistemele SCADA nu se face decat prin cerere aprobata de catre Directorul Tehnic al SC CRAB SA.

Capitolul 6. Măsuri disciplinare

Art. 47. Administratorul reţelei are dreptul să ia măsuri de restricţionare (blocare parţială sau totală), fără notificare, a accesului la Resursele Informatice şi de Comunicaţii în cazul utilizatorilor care încalcă prevederile politicii de securitate şi regulile aplicabile în sistemul de RIC (din planul de securitate) sau legislaţia în vigoare şi care, astfel, pun în pericol funcţionarea şi/sau securitatea reţelei companiei.

Art. 48. Toate acţiunile care contravin legilor vor fi raportate organelor competente.

Capitolul 7. Dispoziţii finale

Art. 49. Prezentul Regulament intră în vigoare la data de 09.12.2024, odată cu aprobarea acestuia de către Directorul General al S.C. COMPANIA REGIONALA DE APA BACAU S.A.