R O M Â N I A
MINISTERUL APĂRĂRII NAȚIONALE
ACADEMIA NAVALĂ "MIRCEA CEL BĂTRÂN"
SENATUL UNIVERSITAR
Nr. H- 697 din 02.11.2023

REGULAMENTUL
PRIVIND POLITICILE DE SECURITATE IT

Preşedinte: Conf. univ. dr. ing. Băutu Andrei
Conf. univ. dr. Popa Cătălin
Prof.univ. dr. ing. Nicolae Florin- Marius
Conf. univ. dr. ing. Deliu Florenţiu
Student Iacobescu Andreea Theodora
Comandor Bucur Eugen
Comandor Bucur Marius

Aviz juridic
Lt. Col.(jurist) Ivanov Georgiana

Capitolul 1. Dispoziții generale

Art. 1. În acord cu prevederile prezentului regulament, Resursele Informatice şi de Comunicații puse la dispoziție şi administrate de către Oficiul pentru Tehnologia Informației și Securitate Informatică sunt bunuri strategice ale Academiei Navale „Mircea cel Bătrân" din Constanța (ANMB);

Art. 2. Documentele interne de reglementare a utilizării Resurselor Informatice şi de Comunicații sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informației şi comunicațiilor în ANMB;

Art. 3. Acestea au ca scop principal protejarea utilizatorilor și a colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea, acestea vizează protejarea datelor stocate în format electronic, a imaginii ANMB şi a investițiilor acesteia pentru dezvoltarea sistemului informatic şi de comunicații;

Art. 4. Rețeaua informatică a ANMB sprijină procesul de învățământ şi de cercetare prin mijloacele de comunicare şi serviciile specifice oferite de rețelele de calculatoare;

Art. 5. Compromiterea securității acestor resurse poate afecta capacitatea ANMB de a oferi servicii informatice şi de comunicații, poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilității instituției în fața partenerilor săi. Prin urmare, prezentul regulament este motivat tehnic de necesitatea menținerii în funcțiune, în condiții de securitate, a rețelelor existente în ANMB, precum şi de necesitatea dezvoltării normale a unei resurse de informare;

Art. 6. Scopul urmărit de politica de securitate este acela de asigurare a integrității, confidențialității, disponibilității, autenticității și nonrepudierii informației, precum şi stabilirea cadrului necesar pentru elaborarea regulilor şi procedurilor de securitate;
(1) *Confidențialitatea* se referă la protecția 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 ANMB sunt proprietatea ANMB în condițiile legilor în vigoare. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la Resursele Informatice şi de Comunicații;
(2) *Integritatea* se referă la măsurile şi procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate;
(3) *Disponibilitatea* se asigură prin funcționarea continuă a tuturor componentelor Resurselor Informatice şi 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 şi de Comunicații;
(4) *Autenticitatea* reprezintă asigurarea că datele, tranzacțiile, comunicațiile sau documentele (în format electronic sau fizic), sunt autentice. De asemenea, este important de a se valida faptul că ambele părți implicate sunt cine pretind a fi;
(5) *Nonrepudierea* reprezintă măsura prin care se asigură faptul că, după emiterea/recepționarea unei informații într-un sistem de comunicații securizat, expeditorul/destinatarul nu poate nega, în mod fals, că a expediat/primit informațiile în cauză.

Capitolul 2. Documente de referință

Art. 7. Legislație primară
(1) Orice activitate care se desfășoară prin intermediul rețelelor existente în ANMB trebuie să respecte legislația în vigoare (internă şi internațională):
- Legea nr. 8/1996, privind dreptul de autor şi drepturile conexe;
- HG 58/1998 – pentru aprobarea Strategiei naționale de informatizare şi implementare în ritm accelerat a societății informaționale şi a Programului de acțiuni privind utilizarea pe scară largă şi dezvoltarea sectorului tehnologiilor informației în România;
- Legea nr. 544/2001 privind liberul acces la informațiile de interes public;
- HG 1609/2008 privind organizarea şi funcționarea Agenției ARNIEC/RoEduNet;
- Convenția privind Criminalitatea Informatică a Consiliului Europei;
- Declarația privind libertatea comunicării pe Internet a Consiliului Europei;
- Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);

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

Art. 8. Reglementări interne - Regulamentele şi procedurile în vigoare în cadrul ANMB.

Capitolul 3. Definiţii

Art. 9. *Intranet* = rețeaua internă de calculatoare;

Art. 10. *Cont* = o entitate specificată printr-un identificator şi o parolă pentru accesul la sistemul de comunicație şi/sau la o resursă de calcul;

Art. 11. *Utilizator* = o persoană, o aplicație automatizată sau proces utilizator autorizat de către ANMB, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele IT;

Art. 12. *Resurse IT* = toate dispozitivele de tipărire/imprimare, dispozitive de afișare, unități de stocare, şi 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, dar nu limitat la: mainframeuri, servere, calculatoare personale, calculatoare-agendă (*notebookuri*, *laptop*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), tablete, sisteme de procesare distribuită, echipament de laborator şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afișa şi transmite informația.

Art. 13. *Administratorul de sistem/Administratorul de rețea* = persoana responsabilă la nivelul instituției cu administrarea Resurselor IT;

Art. 14. *Abuz de privilegii* = orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele ANMB şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acțiunii respective.

Art. 15. *Furnizor*: Persoană fizică/juridică care oferă bunuri sau servicii ANMB în baza unui contract comercial sau de colaborare.

Capitolul 4.

4.1. Politica de securitate

Art. 16. 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 Comunicații ale ANMB şi să instruiască utilizatorii care au dreptul de folosire a Resurselor Informatice şi de Comunicații privind responsabilitățile asociate unei astfel de utilizări.

Art. 17. Clasificarea informațiilor din punct de vedere al securității şi integrității informațiilor:

(1) Informații Publice - acestea sunt informații accesibile oricărui utilizator din interiorul sau exteriorul ANMB. Exemplu de astfel de date sunt cele de la avizier, pe site-urile Web, sau informațiile de presă.
(2) Informații Secrete - aceste informații includ date care dacă sunt făcute publice aduc daune economice sau de imagine ANMB. Astfel de date pot fi: clauze contractuale, informații obținute prin participare la licitații, conturi sau parole etc. Aceste date trebuie protejate prin clauze de confidențialitate.
(3) Informații Strict Secrete - în această categorie intră date ce nu pot fi copiate, distribuite sau șterse fără acordul scris al Conducerii ANMB și care ar aduce mari prejudicii în caz de compromitere. Exemplu: parole la servere, date examene de admitere, chei de criptare etc.

4.2. Audiență

Art. 18. Politica de securitate a resurselor IT în anmb din Constanța se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicații a instituției.

Art. 19. Următoarele entități şi utilizatori sunt vizați în mod distinct de prevederile Politicii:
(1) Angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informațional şi de comunicații;
(2) Studenții ANMB;
(3) Colaboratorii ANMB care au acces la resursele IT;
(4) Furnizorii ANMB care au acces la resursele IT;
(5) Alte persoane, entități sau organizații care au acces la resursele IT.

4.3. Atribuții si obligații

Art. 20. Administratorii rețelei, reprezentați prin specialiști din Oficiul pentru Tehnologia Informației și Securitate Informatică al ANMB, au următoarele atribuții cu privire la Politicile de Securitate:
(1) Aplică şi propun modificări ale Politicii de Securitate;
(2) Elaborează și propun pentru aprobare regulamentele și procedurile de securitate;
(3) Tratează incidentele de securitate;
(4) Elaborează proceduri specifice pentru stabilirea fluxului informațional, accesul la servere și date, backup date etc.

Art. 21. Atribuțiile utilizatorilor sunt:
(1) Să cunoască și să respecte prevederile Politicii de Securitate;
(2) Să cunoască și să respecte prevederile regulamentelor şi procedurilor de securitate;
(3) Să răspundă direct de securitatea şi conținutul informațiilor, precum și de resursele informatice şi de comunicații încredințate direct sau indirect.

Art. 22. Toți partenerii ANMB trebuie să accepte și să respecte aceste politici de securitate.

4.4. Confidențialitatea informațiilor

Art. 23. Fiecare utilizator este responsabil în mod direct de modul de utilizare a resurselor ANMB;

Art. 24. Prin utilizarea serviciului de mesagerie electronică, accesul la informații, navigare Web, acces la rețelele Wireless şi alte instrumente de conversație electronică din cadrul Resurselor Informatice şi de Comunicații ale ANMB, utilizatorul își exprimă acordul implicit privind accesarea datelor personale și monitorizarea în scopul unor investigații sau al rezolvării unor plângeri, în condițiile legilor în vigoare.

Art. 25. Modul de acces la resursele ANMB trebuie reglementat și monitorizat împotriva întrebuințării greșite sau rău voite;

Art. 26. Orice sistem din proprietatea ANMB trebuie să fie însoțit de Fișa Sistemului Informatic și de Comunicații care conține licențele și aplicațiile ce pot fi folosite pe acesta;

Art. 27. Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația şi datele sunt proprietatea ANMB şi trebuie să fie protejate.

Art. 28. Oficiul pentru Tehnologia Informației și Securitate Informatică al ANMB își rezervă dreptul de a șterge, de pe orice sistem orice program sau fișier ce nu are legătură cu scopul muncii respective, sau contravine politicilor ANMB. De asemenea, se poate suspenda funcționarea oricărui echipament care poate afecta funcționarea sistemelor din cadrul ANMB;

Art. 29. Personalul autorizat poate revizui sau utiliza orice informație stocată sau transportată prin sistemele ANMB, în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor (de exemplu, dar fără a se limita la, site-uri web vizitate).

Art. 30. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor
din cadrul ANMB, orice incident de posibilă întrebuințare greșită sau încălcare a acestui regulament.

Art. 31. Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele
ANMB pentru care nu au autorizație sau consimțământ explicit;

Art. 32. Niciun utilizator al sistemelor din ANMB nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemului. Această regulă se extinde şi după ce utilizatorul a încheiat relațiile cu ANMB;

Art. 33. Informațiile publicate electronic de către ANMB pe site-ul propriu *https://www.anmb.ro* şi în subdomeniile acestuia sunt proprietate a ANMB. Caracterul public al acestora reflectă faptul că ele sunt puse la dispoziție de către ANMB în beneficiul comunității publice, în scop de informare asupra programelor academice şi a activității ANMB;

Art. 34. Orice utilizare a informațiilor de pe site-urile publice ale ANMB de către persoane particulare sau organizații în alte scopuri decât cele în care au fost oferite, se face pe propria răspundere a acestora. Într-o asemenea eventualitate, ANMB își rezervă dreptul de a solicita aplicarea prevederilor legale în vigoare;

Art. 35. Fișierele electronice create, trimise, primite sau stocate folosind Resursele Informatice şi de Comunicații administrate sau în custodia şi sub controlul ANMB nu au caracter personal şi pot fi accesate oricând de către specialiștii autorizați din cadrul OTISI, fără înștiințarea utilizatorului.

Capitolul 5.

5.1. Proceduri operaționale de securitate

Art. 36. Politica de securitate a ANMB impune dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau reguli specifice care să asigure integritatea, confidențialitatea, disponibilitatea, autenticitatea și nonrepudierea informației în utilizarea RIC;

Art. 37. Procedurile operaționale de securitate conțin toate regulile aplicabile în sistemul Resurselor Informatice şi de Comunicații ale ANMB;

Art. 38. Procedurile operaționale de securitate au ca scop principal protejarea utilizatorilor şi colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea, acestea au ca scop protejarea imaginii ANMB şi a investițiilor acesteia pentru dezvoltarea sistemului informatic şi de comunicații, protejarea proprietății intelectuale şi a tuturor informațiilor stocate şi transportate cu ajutorul Resurselor Informatice şi de Comunicații ale utilizatorilor autorizați: cadre didactice, personal militar, personal administrativ, studenți, colaboratori etc;

Art. 39. Regulile au fost elaborate pentru fiecare activitate specifică domeniului şi au fost concepute în așa fel încât fiecare să poată fi folosită cvasi independent de celelalte;

Art. 40. Regulile din procedurile operaționale de securitate au rolul:
(1) de a fi corecte, echitabile şi eficiente pentru folosirea resurselor informatice și de comunicație în vederea sprijinirii procesului didactic şi al cercetării științifice;
(2) de a educa utilizatorii resurselor informatice și de comunicație în ceea ce privește responsabilitățile asociate cu utilizarea acestora;
(3) de a fi compatibile cu regulamentele, statutul şi atribuțiile stabilite pentru administrarea resurselor informatice şi de comunicații.

Art. 41. Regulile de utilizare a Resurselor Informatice şi de Comunicații ale ANMB se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la aceste resurse;

5.2. Procedee și reglementări

Art. 42. Privind accesul la serviciul de mail sunt prevăzute următoarele reguli:

(1)Orice parolă trebuie să fie complexă. Pentru parole se respectă Regulile privind parolele de acces de mai jos. Administratorul serverului de mail, creează contul de mail cu o parola inițială, care va fi schimbată de utilizator la prima accesare a contului;
(2)Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces și datele din acestea;
(3) Utilizatorii nu trebuie să trimită, retrimită sau să primească informații confidențiale sau senzitive ce privesc ANMB, folosind conturi utilizator care nu sunt proprietatea ANMB. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea): Yahoo, Gmail, Hotmail, precum şi adrese de email puse la dispoziție de alți Furnizori de Servicii Internet.

Art. 43. De asemenea, referitor la accesul la serviciul de mail, este interzisă:
(1)Trimiterea de mesaje cu caracter de intimidare sau hărțuire;
(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 identități 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 instituția.

Art. 44. Oficiul pentru Tehnologia Informației și Securitate Informatică al ANMB asigură confidențialitatea datelor personale sau a accesului la informații folosind poșta electronică sau alte instrumente de conversație electronică în limitele competențelor, a posibilităților tehnice existente şi a limitelor impuse de prevederile legale în vigoare.

5.3. Reglementări privind securitatea datelor

Art. 45. Securizarea serverelor se realizează prin următoarele reguli:
(1) Serverele trebuie să fie într-o locație cu acces securizat; accesul este restricționat doar la personalul tehnic autorizat;
(2) Instalarea sistemului de operare dintr-o sursă aprobată;
(3) Setarea/activarea parametrilor de securitate, a protecțiilor pentru fișiere şi activarea jurnalelor de monitorizare;
(4) Dezactivarea sau schimbarea parolelor conturilor predefinite;
(5) Crearea şi utilizarea copiilor de siguranță (backup).

Art. 46. Regulile privind parolele de acces sunt următoarele:
(1) Orice parolă trebuie să fie complexă şi să aibă o lungime minimă de 9 caractere. O parolă complexă este un șir de caractere compus din litere minuscule, majuscule, cifre şi simboluri (%$#&^* …);
(2) Nu folosiți aceeași parolă pentru mai multe conturi;
(3) Evitați să păstrați parole în agende electronice, telefoane mobile;
(4) Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puțin o dată la 90 de zile;
(5) Aveți grijă la facilitatea browser-elor de reținere a parolelor (AutoFill, Remember password) cu atât mai mult atunci când calculatorul pe care lucrați este folosit de mai multe persoane;
(6) Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaților care răspund de securitatea sistemelor informatice;
(7) Dacă se suspectează că o parolă a putut fi divulgată, aceasta trebuie schimbată imediat;
(8) Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parola;
(9) Schimbarea parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:

- utilizatorul se va legitima;
- administratorul va verifica drepturile de acces ale persoanei la contul utilizator;
- utilizatorul va introduce o nouă parolă.

Art. 47. Alte reglementări privind securitatea, cu privire la activități interzise:
(1) Activități comerciale neautorizate;
(2) Trafic masiv de informații sau trafic de informații cu caracter frivol, obscen şi pornografic;
(3) Folosirea unor drepturi de acces la resurse pentru care nu sunt autorizați;
(4) Ștergerea 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 defecțiuni hardware şi software;
(8) Perturbarea traficului rețelei ANMB;
(9) Generarea de trafic neacademic;
(10) Transferuri de materiale care contravin legilor drepturilor de autor (software piratat, filme, muzică, cărți, etc.);
(11) Generarea de spam;
(12) Flood (indiferent de natura acestuia), de exemplu: ping flood;
(13) Răspândirea de aplicații de tip malware: viruși, troieni, viermi, spyware sau altele;

(14) Folosirea de aplicații de tip key-logere;
(15) Modificarea adresei MAC a plăcii de rețea;
(16) Modificarea setărilor pentru IP şi DNS, de către oricine altcineva în afara personalului responsabil din Oficiul pentru Tehnologia Informației și Securitate Informatică al ANMB;
(17) Modificarea conexiunilor tehnicii de calcul față de cele stabilite de către personalul autorizat, la cablarea structurată;
(18) Utilizarea de programe pentru scanarea rețelei, exploit-uri;
(19) Transmiterea de mesaje cu caracter comercial;
(20) Publicitatea cu caracter comercial;
(21) Folosirea de software fără licență pe calculatoarele conectate la rețelele ANMB.

Art. 48. Alte reglementări privind securitatea, cu privire la activități recomandate:
(1) Pentru buna funcționare a serviciului de mail și pentru reducerea timpului de realizare a backup- lui, se recomandă păstrarea sub 80% a gradului de ocupare a spațiului de stocare pentru fiecare utilizator;
(2) Eventualele notificări de ordin tehnic (de exemplu: întreruperea temporară a serviciului de mail, modificări, update-uri etc.) vor fi transmise numai de pe adresa de e-mail oficială a Oficiului pentru Tehnologia Informației și Securitate Informatică;
(3) Utilizatorii să citească și să aplice sfaturile pe care le primesc prin mesajele de informare;
(4) Utilizatorii să nu descarce fișiere și să nu acceseze link-uri din cadrul mesajelor trimise de expeditori necunoscuți.
(5) Redirecționarea oricărui e-mail pe care utilizatorul îl consideră a fi spam pe adresa oficială a Oficiului pentru Tehnologia Informației și Securitate Informatică, pentru a fi blocat pe viitor.

Art. 49. Reguli de administrare a conturilor de e-mail:
(1) Fiecare cont de e-mail creat pe domeniul anmb.ro trebuie să aibă asociat o cerere şi o aprobare corespunzătoare;
(2) Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor 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 stabilite;
(5) Spațiul de stocare pentru fiecare utilizator este limitat, dar acesta se poate mări în urma unor solicitări motivate corespunzător;
(6) Pentru accesarea serviciului de e-mail, se va folosi un browser de pe calculatorul individual al fiecărui utilizator;
(7) La cererea conducerii ANMB, Oficiul pentru Tehnologia Informației și Securitate Informatică trebuie să fie în măsură să furnizeze o listă cu toți utilizatorii (listă de conturi) pentru sistemele pe care le administrează.

5.4. Reglementări privind utilizarea RIC în scopuri personale

Art. 50. În această situație se aplică următoarele restricții:
(1) Utilizarea personală ocazională a serviciilor de poștă electronică și acces internet este restricționată la utilizatorii autorizați şi nu poate fi extinsă la membrii familiilor sau alte persoane. Este interzisă utilizarea în scop personal a telefoanelor, fax-lor, imprimantelor sau copiatoarelor ANMB;
(2) Utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru ANMB;
(3) Utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaților;
(4) Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva ANMB sau prejudicierea, indiferent de formă, a intereselor ANMB;
(5) Este interzisă stocarea mesajelor de e-mail, a mesajelor de voce, a documentelor şi fișierelor personale din cadrul RIC;
(6) Toate mesajele, fișierele şi documentele (incluzând eventualele mesaje, fișiere şi documente personale), localizate în cadrul RIC sunt proprietatea ANMB şi pot fi subiectul unor cereri de verificare/inspectare/accesare de către specialiștii OTISI.

Capitolul 6. Măsuri disciplinare

Art. 51. Administratorul rețelei are dreptul să ia măsuri de restricționare (blocare parțială sau totală), fără notificare, a accesului la Resursele Informatice şi de Comunicații în cazul utilizatorilor care încalcă prevederile politicii de securitate şi regulile aplicabile în sistemul de RIC (din planul de securitate) sau legislația în vigoare şi care, astfel, pun în pericol funcționarea şi/sau securitatea rețelei.

Art. 52. În situații cu totul deosebite, când eventuale acțiuni ale unor utilizatori care, pe proprie răspundere, atentează grav la securitatea rețelei, se pot lua următoarele măsuri:
(1) rezilierea contractului de muncă în cazul angajaților civili;
(2) suspendarea sau exmatricularea în cazul studenților;
(3) încetarea relațiilor contractuale (de colaborare) în cazul contractanților, furnizorilor sau consultanților.

Art. 53. Toate acțiunile care contravin legilor vor fi raportate organelor competente.

Capitolul 7. Dispoziții finale

Art. 54. Prezentul Regulament a fost aprobat în ședința Senatului universitar nr. 792_P din data de 31.10.2023.

COMANDANTUL (RECTORUL)
ACADEMIEI NAVALE „MIRCEA CEL BĂTRÂN”
Contraamiral de flotilă
conf. univ. dr. ing. **Alecu TOMA**

PREŞEDINTELE SENATULUI UNIVERSITAR
Prof. univ. dr. ing.
Beazit ALI