INSTITUTUL NATIONAL DE
CERCETARE – DEZVOLTARE PENTRU
OPTOELECTRONICA

CERT NO.: 09/11337

Str. Atomistilor Nr.409, C.P. MG-5, Cod 077125, Magurele - Ilfov, Telefon/Fax: 021.457.45.22, E-mail:inoe@inoe.ro, http://www.inoe.ro

Regulament funcționare a infrastructurii și sistemelor de calcul din cadrul INOE 2000

1. Introducere

Prin prezentul Regulament este stabilit cadrul pentru a asigura o utilizare în siguranță a echipamentelor de calcul și a rețelelor de comunicare electronică asigurând eficiența și buna funcționare a acestora având în vedere un caracter echitabil la resurse precum și asigurarea unui mediu cât mai sigur pentru păstrarea, generarea sau transferarea informațiilor. Prin intermediul acestuia sunt definiți termenii unei conduite acceptabile incluzând drepturi și obligații din partea tuturor entităților implicate.

Acest regulament este realizat conform cu *Strategia de dezvoltare și Conformare a infrastructurii IT* ce reglementează organizarea arhitecturilor și mecanismelor de securitate pentru implementarea cerințelor prevăzute de regulamentele Europene și legislația națională.

Deoarece resursele informatice și de comunicații implementate pe infrastructura Institutului reprezintă bunuri strategice și furnizează resurse vitale pentru funcționarea Institutului iar compromiterea acestora poate avea atât la consecințe locale (fraude, violarea clauzelor contractuale etc.) precum și expunerea informațiilor ce intră sub reglementarea Directivelor Europene (GDPR și NIS2) ce implementează amenzi ca procente din cifra de afaceri.

Din cauza acestor situații prevăzute în special de cadrul legal a apărut motivarea tehnică pe care se bazează prezentul regulament ce guvernează utilizarea rețelelor informatice și a echipamentelor de comunicații ce asigură dezvoltarea naturală a resurselor de informare critice pentru dezvoltarea durabilă, pe termen mediu și lung.

2. Cadrul legal

Orice activitate care se desfășoară prin intermediul rețelei trebuie să respecte legislația în vigoare (internă și internațională):

- Legea nr. 8/1996 (*republicată*) privind dreptul de autor şi drepturile conexe*);
- Hotărârea nr. 1.259/2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronica, cu modificările și completările ulterioare;
- Legea nr. 455/2001 (*republicată*) privind semnătura electronica;
- Legea nr. 544/2001 privind liberul acces la informațiile de interes public;
- Legea nr. 180/2002 pentru aprobarea Ordonanţei Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, cu modificările și completările ulterioare;
- Legea nr. 365/2002 (**republicată**) privind comerţul electronic;
- Hotărârea nr. 1.308/2002 privind aprobarea Normelor metodologice pentru aplicarea Legii nr. 365/2002 privind comerţul electroni
- Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei;
- Legea nr. 196/2003 (*republicată*) privind prevenirea şi combaterea pornografiei*);
- Legea nr. 64/2004 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică;
- Legea nr. 451/2004 privind marca temporală;
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;
- Legea nr. 140/2012 pentru aprobarea Ordonanţei de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, cu modificările și completărilew ulterioare;
- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, denumită în continuare Legea NIS, transpune în legislația națională Directiva (UE) 2016/1148 (NIS) a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, cu modificările și completările ulterioare;
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice

în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor);

- Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică);

- Ordonanţă de Urgenţă nr. 119 /2020 pentru modificarea şi completarea Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice;

- Legea nr. 11/2022 pentru aprobarea Ordonanţei de urgenţă a Guvernului nr. 104/2021 privind înfiinţarea Directoratului Naţional de Securitate Cibernetică;

- Ordonanţă de Urgenţă nr. 89/2022 privind înfiinţarea, administrarea şi dezvoltarea infrastructurilor şi serviciilor informatice de tip cloud utilizate de autorităţile şi instituţiile publice;

- Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative;

- Ordonanţă de Urgenţă nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil;

- Convenția privind Criminalitatea Informatică a Consiliului Europei;

- Politica și Planul de securitate ale Secretariatului de Stat;

- Declarația privind libertatea comunicării pe Internet a Consiliului Europei, etc.), precum și prezentului Regulament.

3. Termeni specifici

IT/ITC – Information Technology/Information Technology and Communications
este tehnologia necesară pentru prelucrarea (procurarea, procesarea, stocarea, convertirea și transmiterea) informației, în particular prin folosirea computerelor (calculatoarelor electronice);

Internet– Rețea de comunicații globală.

Cont/Entitate
reprezintă echivalentul digital al unui document de identitate ce folosește credențiale pentru a asigura accesul autorizat la resursele computaționale sau de comunicații. El poate fi asociat unei persoane fizice, unui proces automatizat sau al unui proces de comunicații securizate;

Administrator
persoană calificată și autorizată responsabilă pentru gestionarea și monitorizarea echipamentelor computaționale sau de comunciații cu drepturi elevate care poate crea într-o manieră responsabilă conturi și asigna drepturi pe baza politicilor interne de acces.

Resurse Informatice și de comunicații
Ansamblul de dispozitive, echipamente, unități de stocare, sisteme de calcul CPU/GPU/TPU/NPU, banda de internet, echipamente active și pasive de rețea conectate la infrastructura Institutului. Aceasta conține și echipamente mobile și resurse de telecomunicații precum și produsele software achiziționate și folosite în cadrul Institutului.

Stație de lucru
Echipament computațional fix sau mobil pe care utilizatorii își desfășoară activitatea.

Server
Echipament computațional fix ce deservește unul sau mai multe servicii digitale publice.

Utilizator/Entitate
O persoană sau aplicație automatizata autorizat să opereze în interesul Institutului, folosind un set de resurse informatice sau de comunicații. El este în mod obligatoriu identificat folosind un set de credențiale și este creat sau restricționat/șters în baza procedurilor operaționale.

Credențiale
ansamblu de informații ce identifică în mod unic un utilizator sau entitate. Acestea includ, dar nu sunt limitate doar la, nume de utilizator. Parola. Cod de identificare personale (PIN), token criptografic, cartele de acces precum și metodele de rigidizare a acestora (Multifactor Authentication).

Abuz de privilegii
orice acțiune intreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele interne și/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acțiunii respective;

Furnizor
persoană fizică/juridică care oferă bunuri sau servicii. în baza unui contract comercial sau de colaborare încheiat cu Institutul;

Incident de securitate
Situație neprevăzută datorată unor factori interni sau externi care pot duce la indisponibilizarea parțială sau totală a resurselor computaționale și/sau a rețelei de comunicații ce poate avea ca scop extragerea de informații aflate în proprietatea Institutului.

Administrarea incidentului
toate procedurile utilizate pentru detectarea, analiza şi limitarea unui incident de securitate precum şi răspunsul la acesta și mitigarea situațiilor viitoare conform cadrului legal și a reglementărilor în vigoare;

Servicii digitale
Ansamblul de servicii electronice expuse public (pe Internet) ce include pagini web, servicii email etc. furnizate prin mijloace electronice - serviciu transmis iniţial şi primit la destinaţie prin intermediul echipamentului electronic pentru procesarea, inclusiv arhivarea digitală şi depozitarea datelor, şi care este integral transmis, transferat şi recepţionat prin cablu, prin unde radio, prin mijloace optice sau prin alte mijloace electromagnetice;

Furnizor de servicii digitale
Este un furnizor ce asigură servicii digitale ce contribuie la buna funcționare a serviciilor publice oferite de Institut.

Risc
orice circumstanţă sau eveniment ce poate fi identificat în mod rezonabil, anterior producerii sale, care are un efect potenţial negativ asupra securităţii reţelelor şi a sistemelor informatice;

Securitatea reţelelor şi a sistemelor informatice
capacitatea unei reţele şi a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acţiuni care compromite disponibilitatea, autenticitatea, integritatea, confidenţialitatea sau non-repudierea datelor stocate ori transmise sau prelucrate ori a serviciilor conexe oferite de reţeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

Non-repudierea datelor
un serviciu care este utilizat pentru a oferi asigurarea integrității și originii datelor în așa fel încât integritatea și originea să poată fi verificate și validate de o terță parte ca provenind de la o anumită entitate care deține cheia privată (adică, semnatar);

4. Cadru general

Pentru asigurarea bunei desfășurări a activității Institutului, prezentul regulament asigură cadrul necesar pentru utilizarea resurselor informatice aflate în proprietatea Institutului.

4.1 Reglementări generale

1. Utilizatorii trebuie să cunoască principiile de Operare a sistemelor de calcul și să realizeze independent activitățile legate strict de operare. Pentru activitățile ce necesită drepturi administrative trebuie să apelați la persoanele autorizate.
2. Odată cu reglementările strict furnizate de regulamentele Europene, pentru orice stație de lucru, este obligatoriu ca accesul să fie realizat folosind strict credențiale care să identifice în mod unic utilizatorii ce au realizat operațiile respective. În consecință, toate stațiile de lucru trebuie să nu permită în niciun fel accesul utilizatorilor generici de tip guest sau fără credențiale.
3. Credențialele, cu excepția sistemelor bazate pe stampa de timp (token-uri criptografice sau Multi-Factor Authentication) trebuie modificate la un interval de timp de maxim 90 de zile.
4. Este interzisă partajarea/comunicarea credențialelor cu alte persoane din cadrul sau dinafara Institutului.
5. În cazuri speciale, conform Directivei GDPR, accesul la conturile de utilizator ale altor persoane pote fi obținut în regim de urgență, cu ajutorul unui referat aprobat de către conducerea Institutului. În aceste situații, personalul administrativ va schimba credențialele pentru utilizatorul respectiv și acestuia îi vor fi comunicate noile credențiale cât mai curând posibil.
6. Este interzisă modificarea, reinstalarea sau evitarea sistemelor de control al accesului precum și alte activități de către alte persoane decât cele autorizate.
7. Este interzisă modificarea, comunicarea sau ștergerea de date sau de informații altele decât a utilizatorului responsabil pentru acele date.
8. La părăsirea Institutului, conținutul și informațiile păstrate pe resursele computaționale vor fi transferate către o altă persoană din cadrul Institutului urmând ca în 60 de zile contul de utilizator și toate informațiile aferente acestuia să fie șterse.
9. Atunci când utilizatorii stațiilor de lucru au drepturi administrative, răspunderea asupra programelor instalate și a legalității acestora cade în totalitate asupra utilizatorului respectiv.
10. Utilizatorilor le este interzis să se angajeze în acțiuni împotriva scopurilor INOE 2000.
11. Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale impotriva INOE 2000 sau prejudicierea, indiferent de formă, a intereselor acestuia.
12. Toate mesajele, fișierele și documentele localizate în cadrul RIC sunt proprietatea INOE 2000 și pot fi subiectul unor cereri de verificare/inspectare/ accesare conform regulamentelor.
13. Este interzisă realizarea de activități ce sunt sau pot fi interpretate ca atacuri, scanări sau încercări de exploatare a vulnerabilităților sistemelor informatice. Astfel de verificări se realizează de către furnizori de servicii digitale de securitate informatică autorizați.

4.2. Utilizarea resurselor informatice

1. Utilizarea resurselor computaționale se face numai în interes de serviciu.
2. Este interzisă realizarea de activități recreative (accesarea rețelelor sau site-urilor de divertisment, jocuri etc.).
3. Este interzisă utilizarea resurselor computaționale în scopul obținerii de foloase personale.
4. Utilizatorilor le este interzis să acceseze, să creeze, să stocheze sau să transmită materiale pe care INOE 2000 le poate considera ofensive, indecente sau obscene.
5. Utilizatorilor le este interzis să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală și a dreptului de autor (copyright).
6. Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale impotriva INOE 2000 sau prejudicierea, indiferent de formă, a intereselor acestuia.
7. Prin actiunile lor, utilizatorii 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 și disponibilitatea informațiilor de orice tip.
8. Fiecare stație de lucru trebuie să ruleze soluția antivirus/EDR agreată și achiziționată de conducerea unității. Este interzisă oprirea temporară sau permanentă a acesteia.
9. Este interzisă instalarea de produse software ale căror sistem de licențiere nu este destinat instituțiilor (de exemplu versiunile Home ale sistemului de operare Windows).
10. Utilizatorilor le este interzis să instaleze sau să utilizeze produse software sau componente ale produselor software pentru care Institutul nu deține licență.
11. Utilizatorilor le este interzis:
    - să se angajeze într-o activitate care ar putea hăitui sau amenința alte persoane;
    - să degradeze performanțele sistemelor informaționale;
    - să împiedice accesul unui utilizator autorizat;
    - să obțină alte resurse în afara celor alocate;
    - să nu ia în considerare măsurile de securitate impuse prin regulamente.
12. Utilizatorilor le este interzis să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității sistemelor. De exemplu, utilizatorii INOE 2000/ filiale INOE 2000 nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.
13. Utilizatorii care au acces la resursele informatice ale INOE 2000 au obligația de a purta acte și/sau legitimații care să ateste calitatea de utilizator autorizat în spațiile instituției.

4.2. Utilizarea echipamentelor externe

În situații specifice în care sunt introduse în sistemul informatic echipamente externe cum ar fi calculatoare personale, echipamente ale echipelor de service pentru dispozitive științifice, utilizarea telefoanelor personale folosind rețelele Wifi etc. trebui avute în vedere următoarele reguli:

1. Utilizarea resurselor de comunicare (de exemplu a adreselor IP pentru accesarea de reviste științifice) presupune identificarea Institutului și poate aduce consecințe asociate acestui aspect.

2. Utilizarea sistemului de email, a fax-urilor sau a oricăror echipamente ale Institutului pentru transmiterea de informații personale sau în interesul unor terțe părți trebuie aprobate de conducerea Institutului.
3. Utilizarea nu trebuie să aibă drept rezultat costuri directe pentru INOE 2000;
4. Utilizarea nu trebuie să afecteze activitatea normală a angajaților.

5. Servicii publice găzduite.

O parte a serviciilor digitale furnizate prin intermediul infrastructurii Institutului necesită acces public și administrare din partea personalului științific. În această categorie intră paginile web de proiect ale căror administrare intră în sarcina managerului de proiect. Pentru acestea:

1. Echipele tehnice asigură funcționarea și disponibilitatea paginii;
2. Conținutul și informațiile publicate intră în sarcina persoanei ce administrează pagina și nu pot fi modificate de personalul tehnic decât în situație de urgență;
3. Pentru fiecare astfel de aplicație este desemnat câte un administrator, adică acea persoană care primește credențialele inițiale de administrare;
4. Credențialele inițiale trebuie să fie imediat înlocuite cu credențiale cunoscute doar de persoana ce administrează paginile și sunt impuse condițiile de reglementare asociate credențialelor (complexitate, netransmitere către terți etc.);
5. Este interzisă utilizarea de credențiale care să fie ușor de ghicit de către persoane externe;

6. Recomandări privind credențialele

1. Este recomandată utilizarea de sisteme de tip password manager care să permită și delegarea în situații de urgență;
2. Este recomandată nereutilizarea parolelor (pentru a evita compromiterea pe lanț);
3. Este recomandată utilizarea sistemelor de autentificare multifactor (MFA/2FA) acolo unde este posibil;
4. Este recomandată utilizarea sistemelor de autentificare moderne, de tip passwordless acolo unde este posibil;

O soluție în acest sens este disponibilă la nivelul Institutului.

7. Raportarea activităților anormale sau suspecte

Infrastructura publică este în permanență supusă atacurilor informatice ale căror scop poate să fie obținerea de informații, indisponibilizarea infrastructurii sau chiar distrugerea acesteia. Deoarece, în ultimii ani au fost întâlnite mai multe vulnerabilități de tip 0-day exploatate iar soluțiile de securitate să nu cunoască încă aceste vulnerabilități iar modelele statistice de identificare a anomaliilor să fie evitate, intră în rolul fiecărui utilizator să anunțe, de preferință pe canale rapide de comunicație astfel de suspiciuni.